(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2001 (21.06.2001)

PCT

(10) International Publication Number
WO 01/45350 A2

(51) International Patent Classification⁷: H04L 29/00

(21) International Application Number: PCT/US00/42601

(22) International Filing Date: 6 December 2000 (06.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/172,494	17 December 1999 (17.12.1999)	US
60/173,938	30 December 1999 (30.12.1999)	US
60/182,958	16 February 2000 (16.02.2000)	US
09/606,579	29 June 2000 (29.06.2000)	US

(71) Applicant: DATASAFE, INC. [US/US]; 30-31 Union Wharf, 1st Floor, Boston, MA 02109 (US).

(72) Inventors: MULLER, David, F.; 87 Chestnut Street, Boston, MA 02108 (US). GRUNDY, Adrian, R.; 418 Glen Road, Weston, MA 02493 (US).

(74) Agents: ROOS, Richard et al.; Nutter, McClennen & Fish, LLP, One International Place, Boston, MA 02110-2699 (US).

(81) Designated States *(national)*: AU, CA.

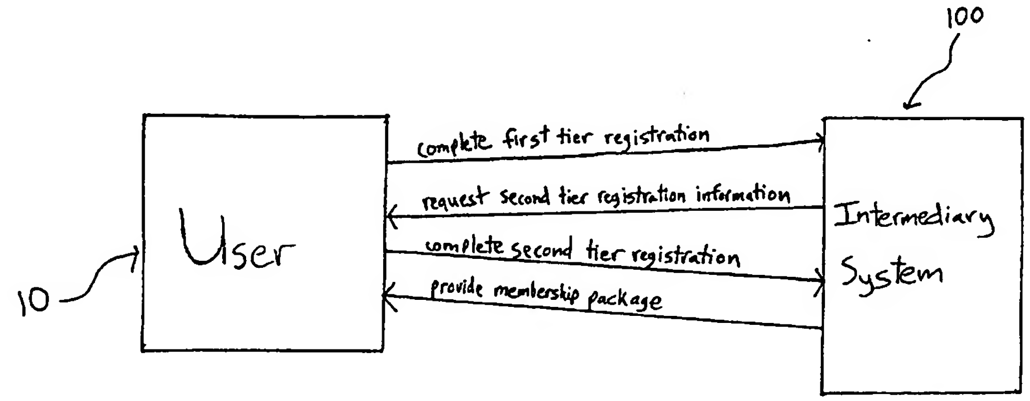
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COMMUNICATIONS NETWORK INTERMEDIARY SYSTEM


100
complete first tier registration
request second tier registration information
complete second tier registration
provide membership package
User
Intermediary System
10

(57) Abstract: The present invention provides an intermediary system that allows a first party to anonymously browse and conduct transactions on a communication network, such as the Internet. In one embodiment of the present invention, a user utilizes the system to anonymously browse the Internet and then to indirectly purchase items from one or more vendors at one or more Internet sites. The intermediary system acts as an intermediary between the user and the vendor(s) in order to provide an added level of security and to maintain the privacy of the user during the transaction. The intermediary system can also interact with other parties, such as a financial institution, a shipping company, and/or a package depot, in furtherance of a transaction while preserving some or all of the user's privacy and security.

WO 01/45350 A2

COMMUNICATIONS NETWORK INTERMEDIARY SYSTEM

FIELD OF THE INVENTION

The present invention relates generally to security and privacy systems useful with communications networks and with electronic transactions, including electronic commerce.

BACKGROUND OF THE INVENTION

There has long been a need for security in virtually any communications network on which various forms and types of data are transferred from one network site to another. In response, many security features have been implemented in an attempt to ensure that communications and data transfer over such networks are secure. Examples of such security features include specialized access cards, passwords, and biometrics.

A relatively new communications network is the "Internet," which has enjoyed an enormous rise in popularity, use, and applicability in recent years. The Internet is used for entertainment and information retrieval purposes, as well as to effectuate business and commercial transactions. Use of the Internet, however, frequently entails a risk that information about the Internet user will be revealed as a result of the user browsing and/or engaging in Internet-based transactions such as electronic commerce. The information revealed can include personal information (e.g., a user's identity), a user's browsing habits, its purchasing preferences and patterns, as well as the user's credit and/or financial information about the user.

It is well known, in fact, that personal information and browsing habits regarding Internet users are of great value to Internet businesses. This has prompted Internet businesses to seek out companies that provide Internet user profiling data . This data usually consists of aggregated statistics of the browsing patterns and habits of web-site users and visitors. Internet businesses crave such data as it greatly facilitates their ability to target potential on-line purchasers.

Because of the widespread use of the Internet, its enormous economic potential, and this ability to mine information about Internet users and their usage habits, Internet privacy is a significant concern to the general public and governmental agencies alike.

Many consumers are so reluctant to disclose personal information, that their use of the full potential of the Internet has not been realized.

The growth of electronic commerce has also heightened concerns from Internet users and business alike regarding Internet security. Annual revenue derived from on-line shopping amounted to $8 billion in 1998, a figure that is expected to grow to $45 billion by 2001, and to over $80 billion by 2003. With this increasing level of electronic commerce activity,. there is likely to be a concurrent increase in fraud as a result of the interception and misuse of credit information (e.g., credit card numbers) by unauthorized third parties. This is troublesome because, according to Visa International, the Internet already accounts for one-half of credit card disputes and fraud incidents despite the fact that less than 2% of the overall business of credit card companies is derived from Internet transactions.

If the true potential of the Internet as a vehicle for electronic commerce is to be realized, systems are needed to ensure the privacy of Internet users. There is also a further need for systems that increase Internet security so that incidents of fraud on the Internet can be significantly reduced, if not eliminated altogether.

SUMMARY OF THE INVENTION

The present invention provides a method for facilitating anonymous access to one or more locations on a communications network. In one aspect of the invention, a first party or user accesses an intermediary via the communications network at an intermediary host site. The user instructs the intermediary to connect to a second party site, which may be an e-commerce vendor site, on the communications network. The user may then access and browse the second party site through this connection without the second party being able to detect the user's identity.

In another aspect of the invention, a user may anonymously engage in an electronic commerce transaction with at least one vendor site on the world wide web. The user accesses an intermediary host site that has an Internet Protocol (IP) address on the world wide web. The intermediary relabels any headers, identifiers and IP addresses contained in data packets submitted by the user in connecting to the intermediary host site. The user, through the intermediary, is then connected to a desired vendor site that also has an IP address on the world wide web. The user may then access and purchase one or more items from the vendor site through this connection without the vendor being able to detect the user's identity. In one embodiment, further privacy may be obtained by encrypting Universal Resource Locators (URLs) to provide a secure channel connection between the user and the intermediary. This level of privacy will even prevent the user's Internet Service Provider (ISP) from detecting the site visited by the user.

In yet another aspect of the invention, a user may register with an intermediary to engage in electronic commerce transactions while maintaining the user's privacy. The intermediary has a host site on the Internet at which users can register to become authorized members of the intermediary host site. A user is allowed access to the intermediary host site upon providing predetermined identity verification data to the intermediary that is sufficient to establish that the user is an authorized member. The intermediary, as noted above, scrubs the data packets forwarded by the user's connection to the intermediary host site, allowing the user to connect to a desired vendor site on the Internet anonymously. The host site then forms such a connection, grants the user electronic and visual access to this connection, and enables the user to purchase one or more items from the vendor site, without the vendor site being able to detect the user's identity.

The invention also provides methods and techniques for protecting a user's identity and privacy during the shipment of goods.

For the sake of convenience, the terms "Internet" and/or "world wide web" are used herein to encompass the global network commonly known as the Internet, as well as intranets, LANs, WANs, dial-up or other types of electronic bulletin boards, or any other wired or wireless communication network(s) or media. The term "communications network" encompasses any system over which a party can communicate voice and/or data signals to another party. This term encompasses, for example, computer networks such as the Internet, and telephone networks. Also, the term "computer" is used herein to encompass any type of computer known in the art, as well as any other device (e.g., cell phone, pager, television set) that permits communication over the "Internet" as defined herein.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be more fully understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a schematic block diagram depicting a process in which a user registers with an intermediary system in accordance with the present invention;

FIG. 2 is a schematic block diagram depicting a process in which the user connects to the intermediary system;

FIG. 3 is a schematic block diagram of a workstation the user may utilize to connect to the intermediary system;

FIG. 4. is a schematic block diagram depicting the interaction between the user and the intermediary system on a communication network;

FIG. 4A is a schematic block diagram depicting an alternative interaction between the user and the intermediary system on a communication network.

FIG. 5 is a schematic block diagram depicting a one-way firewall between the user and one ore more target Internet sites;

FIG. 6 is a schematic block diagram depicting the split image that a user may receive when connected to the intermediary system;

FIG. 7 is a schematic block diagram of an embodiment of the present invention that depicts a transaction between the user and one or more target sites utilizing the intermediary system;

FIG. 8 is a schematic block diagram of an alternate embodiment of the FIG. 7 embodiment that further involves a shipping company in the transaction;

FIG. 9 is a schematic block diagram of an another alternate embodiment of the FIG. 7 embodiment that further involves a package depot in the transaction;

FIG. 10 is a schematic block diagram of an alternate embodiment of the FIG. 7, FIG. 8 or FIG. 9 embodiments that further involves a financial institution;

FIG. 11 is a schematic block diagram depicting the interaction between the user, the intermediary system, and one or more second parties wherein the user is seeking to return or exchange items ordered in a transaction in accordance with the embodiments of FIG. 7, 8, 9 or 10;

FIG. 12 is a schematic block diagram depicting the interaction between the user, the intermediary system, and the one or more target sites during the return or exchange process of FIG. 11;

FIG. 13 is a schematic block diagram depicting an exemplary split image that a user may receive when connected to the intermediary system;

FIG. 14 is a schematic block diagram depicting another exemplary split image that a user may receive when connected to the intermediary system; and

FIG. 15 is a schematic block diagram depicting yet another exemplary split screen image that a user may receive when connected to the intermediary system.

DETAILED DESCRIPTION OF THE INVENTION

The present invention provides a system that allows communication and data transfer over a communications network, such as the Internet, to occur with enhanced privacy and/or security. In one embodiment, the invention provides an intermediary system that a first party or user utilizes to anonymously browse a communications network and then to indirectly purchase from, or place an order with, one or more vendors via the communication network while maintaining a desired level of anonymity.

Although the invention is primarily described with reference to the Internet being the applicable communications network and the relevant transaction being an electronic commerce purchase, it is understood that the invention is applicable to other communications networks as well. For example, the invention is also applicable to the use of an intermediary system to facilitate mail order and/or telephone order (MOTO) transactions.

To use the intermediary system, a user initially registers with the system. Once registered, the user is able to request connection to the intermediary system (e.g., via a communications network), which will require that the user verify its identity through one or more identification steps. Once connected to the system, a user is able to browse the Internet anonymously. The user does this by submitting site locating information, such as a URL, Internet Protocol (IP) address, or http call, to the system, which removes user-identifying information from the user's data pockets and connects to the one or more target sites on the Internet. The user can monitor and affect each system-to-site connection anonymously. Some or all of this anonymity is maintained if the user subsequently elects to make a purchase from a vendor having a presence on, or connection to, the Internet site(s).

Referring initially to FIG. 1, a schematic block diagram depicts the process whereby a first party or user 10 registers with the intermediary system 100. The user 10 may be any potential user of a communications network (e.g., the Internet) who desires to browse the network and/or to engage in electronic commerce transactions anonymously. An actual user 10 may be one or more individuals or a company.

The registration process may include one step or, preferably, several discrete steps, and occurs either entirely on the Internet or, preferably, partially on the Internet. In an exemplary embodiment of the present invention, the user 10 registers with the intermediary system 100 via a two-tiered registration process. A first step in the registration process commences when the user 10 contacts the system 100 and provides the system with first tier registration information. This first tier registration process generally occurs entirely on-line, but may occur partially or entirely via telephone. Exemplary first tier registration information includes some or all of the name, mailing address and electronic mail address of the user 10. One of ordinary skill in the art will appreciate that additional information may be requested in the first tier registration process.

The system 100 receives and retains this information and then requests second tier registration information from the user 10. In an exemplary embodiment of the invention, the system 100 does this by sending the user 10 a physical package (e.g., via one or more mailings) containing forms, which the user must complete and return to the system. It is understood, however, that this request may be entirely or partially conveyed from the system 100 to the user 10 in other ways, e.g., in electronic form or via telephone questioning.

This second tier registration information includes financial information, and, optionally, further personal information pertaining to the user 10. The financial information can include one or more account numbers of bank accounts of the user 10, and/or debit or credit card data, such as card number, issuing bank, and/or expiration date. The personal information can include, for example, the user's 10 telephone number, social security number and/or predetermined family information.

The user 10 then provides this second tier registration information to the system 100. This may be done, for example, entirely or partially via one or more mailings, electronic communications, or telephone calls. Once received, this information is combined with the first tier information to form the user's registration profile, thus completing the registration process. All of the information that forms the user's registration profile is generally kept in strict confidence by the system.

One of ordinary skill in the art will readily appreciate that the user 10 may only be required to provide some of the first and second tier registration information in order to complete the registration process. Alternatively, the user 10 may need to provide additional information in lieu of, or in addition to, the first and second tier registration information. For example, the user 10 may be required to provide one or more biometric characteristic standards to the system 100 during or following the second tier registration process in order to complete the overall registration process. Such standards are stored by the system for subsequent comparison purposes that will be described in further detail below.

The biometric characteristic may be an ocular-based identification characteristic, such as a partial or complete retinal image, or a partial or complete iris image. Instead, the biometric characteristic may be a manual-based identification characteristic, such as a thumb print, a finger print or a palm print, or a pedal-based identification characteristic, such as a toe print or a foot print. Other exemplary biometric characteristics include, but are not limited to, a voice pattern, a handwriting sample, or a stroke pattern (e.g., a keystroke). Preferably, the biometric characteristic is an ocular-based identification characteristic, most preferably, a partial or complete retinal image of the user 10.

The user 10 may provide the biometric characteristic standard in a variety of ways. Exemplary techniques include, but are not limited to, the use of a device at the user's location, the use of a centrally located device to which the user must travel, and the use of a device that has been loaned or otherwise provided to the user.

Once the registration process is complete, the user 10 is provided with a membership package. This package explains how the user 10 may utilize the intermediary system 100 in conjunction with Internet browsing and/or purchasing. The package will also include an identification token, such as an identification (ID) card.

The ID card is preferably unique to the user 10, and enables the user to identify itself to the system 100 so that the system can, in turn, match the user to its registration profile, and to any or all of the personal or financial information contained within the profile. The ID card may include a code, such as an alphabetical code, a numerical code, or an alphanumeric code, that may be displayed on or embedded in the ID card. Examples of codes that are embedded in the ID card include machine readable codes, such as codes embedded in a magnetic strip, bar codes, and computer chips (e.g., RF chips).

The ID card may optionally include one or more security features. For example, the card may include a component (e.g., a chip) that produces a time-variable code. This code, like the PIN, may be entirely or partially numeric or letter-based. In an exemplary embodiment, the code is entirely numeric, and has a non-predictable value that entirely or partially changes within a predetermined time increment. Preferably, the code entirely changes within approximately a one second to about a five minute time increment. Most preferably, this value entirely changes approximately every thirty to sixty seconds. The code appears to be randomly generated, but it is controlled and predictable by an algorithm under the control of the system. The system 100 is adapted to possess or otherwise have access to this code at any given date and time in a manner that is generally known in the art, such as by having the same synchronized chip or access to a master code reader.

The process in which such a code is generated, as well as the control logic used to generate it, are generally known in the art. For example, the algorithm described in U.S. Patent No. 4,720,860 to Weiss, which is expressly incorporated by reference herein, can be utilized to generate such a time-variable code.

The membership package also will generally contain a temporary personal identification number (PIN) that is linked to the ID card and other user information which the user 10 will need to provide in order to access the system 100. The user 10 can opt to continue to use this temporary PIN, or can change it to another PIN. As used herein, the terms "Personal Identification Number" and "PIN" are understood to refer to code that may be alphabetical, numeric, or alphanumeric.

Referring now to FIG. 2, once the user 10 receives its membership package, it can request to connect to the intermediary system 100. The user 10 may do so, for example, via a communication network through the use of a computer 20 as is generally known in the art. Upon receiving the user's 10 request for connection, the system 100 will prompt the user to supply predetermined log in authentication information as a security feature to enable the system to confirm that the user is actually the individual or entity he, she or it purports to be.

In one embodiment, the system 100 requires a two-factor user authentication. The first factor is the user's PIN, and the second factor is the ID card code, each as described above. The user 10 conveys the requested authentication information to the system 100 via its computer 20 that is linked to the system over the communications network as is generally known in the art. In another embodiment, the system 100 requires a three-factor user authentication in which the user 10 is required to provide the two authentication factors discussed above, plus additional information, such as a biometric characteristic sample. In such an embodiment, the user 10 will have already provided the system with a biometric characteristic standard as discussed above. A suitable biometric characteristic sample is obtained at the time of attempted user 10 log in, and is compared against the previously supplied biometric characteristic standard to authenticate the user's identity.

It is understood, of course, that the invention also covers an embodiment in which the system only requires that the user 10 provide a single factor authentication in response to a user log in request. In such an embodiment, the single factor may be any of the three factors discussed above or an alternative authentication factor.

FIG. 3 schematically depicts a user workstation 30 that is adapted to obtain and transmit a biometric characteristic sample of the user 10 to the intermediary system 100 in accordance with a user log in procedure. The workstation 30 generally includes at least a biometric characteristic obtainment device 40 and a computer 20. The device 40 is preferably portable, mountable on, or connectable to the computer 20. The device 40 also has access to a communications network, such as the Internet, through its connection to the computer 20. In one embodiment, the device 40 can be mounted on or attached to a computer monitor (not shown) associated with the computer 20.

In use, the biometric characteristic obtainment device 40 may function as follows. The device 40 receives a signal 50 from the computer 20 instructing it to obtain a biometric characteristic sample from the user 10. The signal 50 can emanate from the user 10, such as via a keystroke or voice instruction. Alternatively, the signal can emanate from a separate party, such as the intermediary system 100 via a signal transmitted through the communications network.

The computer 20 processes the signal 50 via a processor 60, and forwards the signal to the device 40. Once the device 40 receives and reads the signal 50, it either prompts the user 10 to activate the device to produce a biometric characteristic sample, or automatically causes the device to activate and to obtain biometric characteristic sample of the user.. The biometric characteristic sample is then converted to an electronic signal (e.g., a digital signal) in a manner well known in the art, and then is transmitted to the system 100 or another party as discussed below.

Although the device 40 may be any type of biometric characteristic sample obtainment device, in an exemplary embodiment of FIG. 3, the device 40 is a retinal scanning device (such as a camera) that records a digital image of at least part of the user's retina and/or of another part of the user's eye. The retinal scanning device 40 may be of any type known in the art; illustrative retinal scanning devices are shown and described in U.S. Patent Nos. 5,861,938 and 5,861,939, each of which is expressly incorporated by reference herein.

In general, retinal scanning devices obtain an image of at least a part of the retina of an eye. This may be accomplished, for example, by using light (e.g., diode light) to generate the retinal image. As is well known to one of ordinary skill in the art, the retina provides a unique vasculature pattern that can be used to verify the identity of an individual. The pattern can be coded using conventional techniques to reduce the space required to store the pattern. It is also understood that pattern resolution can be varied to achieve a desired confidence level for the verification process. A retinal scanning device 40 can be readily adapted for non-permanent mounting on, and connection to, the computer 20 or a computer monitor (not shown) to obtain a digital image of the user's retina using a retinal image gathering component 70 of the device.

It is understood that to ensure proper use of a retinal scanning device 40, the computer 20, or any components of the workstation 30, some level of training and/or instruction may be advisable.

FIG. 3 also illustrates that the biometric characteristic obtainment device 40 may contain a component 80 (e.g., a chip) that assigns at least one additional identifier code to the produced biometric characteristic sample. This additional identifier code can be any piece of information capable of serving as an additional identifier of the produced biometric characteristic sample. For example, the additional identifier can be a time-varying code, such as the code of the ID card. As stated above, such a time-variable code may be generated as is generally known in the art, such as via the algorithm and process described in U.S. Patent No. 4,720,860 to Weiss. In one embodiment, the additional identifier has a different value than the ID card's code and it is neither known to, nor controllable by, the user.

The component 80 is electronically or otherwise coupled to the biometric characteristic sample obtainment device 40. This enables the biometric characteristic sample data to have imbedded therein, or coupled thereto, the identifier code that was generated on the date and time that the biometric sample was collected. Once the biometric characteristic sample has been produced and the identifier has been embedded therein or coupled thereto, the device 40 then transmits the gathered information back to the computer 20 via a signal 90 as is generally known in the art. The information transmitted to the computer 20 may include the produced biometric characteristic sample, the date and time that the sample was produced, the identifier value, and/or the date and time the identifier value was obtained.

One of ordinary skill in the art will readily appreciate that the code-generating component 80 need not be incorporated within the biometric data gathering device 40, but instead, may be incorporated within the computer 20. In such an embodiment, the system would be configured to couple the biometric characteristic sample data with the identifier value, as well as with other useful data including the time that the sample data was gathered.

Once the processor 60 obtains and processes whichever information is provided to it by the device 40 and the component 80, this information, which collectively forms an identity profile is transmitted electronically to another party, such as the identity verification system 100. It is understood that the identity profile may be transmitted to other parties instead of or in addition to the system, such as one or more vendors and/or one or more financial institutions.

Once the system 100 receives the identity profile from the user's computer 20, the system compares the information contained within the profile to information that the system has obtained as a result of the registration process. For example, the system 100 compares the biometric characteristic sample component of the identity profile with the stored biometric characteristic standard for the user. If they do not correspond, either exactly or to a predetermined degree of matching, then the system 100 will not verify or authenticate the identity of the user 10, and will not allow the user to connect to the system.

If, however, the biometric characteristic sample and standard correspond either exactly or within a predetermined degree of matching, the system 100 will examine the value of the additional identifier code component of the identity profile to information the system possesses. To do so, the system 100 possesses, or otherwise has access to, the value of the additional identifier code at any given date and time in a manner that is generally known in the art. For example, the system 100 may have the same synchronized chip or access to a master code reader. By comparing both the biometric characteristic sample and the value of the additional identifier, the system is able to add an additional level of access security.

Although the identity verification and security procedures are discussed primarily in the context of gaining access to an intermediary system 100, it is understood that the same procedures are applicable to any system having a need to control or restrict user access over any communications network.

Once the user 10 has provided the intermediary system 100 with the requisite identity verification information, the system will allow the user to connect thereto. It is understood that multiple users 10 may be simultaneously connected to the system 100. Once connected to the system 100, any user 10 may then utilize the system in a desired manner. For example, the user 10 may use the system to assist in browsing the Internet and/or to assist in completing a electronic commerce transaction.

Exemplary browsing processes are depicted in FIGS. 4 and 4A, in which a user 10 utilizes (i.e., navigates or "surfs") a communications network, such as the Internet, to select one or more target site(s) 200 to browse. The user 10 does this by transmitting site locating information, such as a URL, Internet Protocol (IP) address, or http call, to the system 100. The system 100 then relabels this information and connects to the target site(s) 200 either directly, or indirectly, such as through an Internet portal or link. This relabelling process preserves the user's 10 anonymity by preventing the target site(s) 200 from tracing the user 10 to the connection between the system 100 and the target site(s). Once this system 100 to target site(s) 200 connection is established, the system may transmit a clone of the connection to the user 10 as is generally known in the art. In the embodiment illustrated in FIG. 4A, no clone connection is transmitted to the user. Rather, the user connects to the target site 200 through the intermediary 100. It is understood that the target sites 200 may be any sites on the Internet including, but not limited to, entertainment sites, information sites, search engines or portals, or electronic commerce sites.

FIG. 5 depicts an embodiment of the invention in which the system is simultaneously connected to the user 10 and the target site(s) 200. To allow this, while still preserving the user's anonymity, the system utilizes a one-way firewall 300, which prevents the target site(s) 200 from being aware of information that the user 10 transmits to the system 100 prior to that information being relabelled. The firewall 300 does not, however, prevent the user from being aware of the information exchanged between the system 100 and the target site(s) 200. In one embodiment, the system may be simultaneously and separately connected to the user 10 and the target site(s) 200.

The above-described relabelling process and the presence of the firewall 300 together allow the user 10 to communicate anonymously with one or more target site(s) 200 through the system 100. It is understood, however, that the user 10, in certain instances, may want to communicate with the target site(s) 200 through the system 100 indirectly, but without complete anonymity. For example, the user 10 may wish to receive tracing or location assistance information (e.g., cookies) from certain sites 200. If so, the user 10 may provide site management information to the system 100. In such an embodiment, the system 100 compares the cookies offered by each site 200 to the user's site management information to determine whether the user 10 wishes to accept cookies from that particular site. One of ordinary skill in the art will readily appreciate that the user 10 can disable or alter this site management information at any time.

The relabelling of the user information generated by the communication between the user 10 and the system 100 can be effected by changing the headers, identifiers, and IP addresses that are indicative of the user to those indicative of the system 100. This identifying data can be used in any subsequent connections between the system and the target site(s) 200 that are requested by the user. The firewall prevents the target site from ascertaining the true identity of the user.

One of ordinary skill in the art will understand that various techniques and technologies are available to effect anonymous browsing on the Internet. For example, a user may be connected to a target website through an intermediary, such as the system described herein, without the target site perceiving the user's identity. Further protection is available to provide a secure channel between the user and the system. This enables the URL to be encrypted so that user identity information is concealed from the user's Internet Service Provider (ISP) as well as any unauthorized thirty party. It is understood that any such technique and technologies may be used with the present invention.

Once the system 100 is connected to the target site(s) 200, the user 10 should receive notification of that connection by direct viewing of the connection or via a clone image of the connection. Generally, if a clone image is used, this notification and the clone image are transmitted to the user's computer screen or monitor. In one embodiment, shown in FIG. 6, the user's 10 computer screen 400 has a split image, including a first image 400A that displays the connection between the user 10 and the system 100, and a second image 400B that displays the clone of the information exchanged via the connection between the system and the target site(s) 200. These screen images 400A, 400B are updated continuously as the user 10 communicates with the system 100, and as the system, in turn, communicates with each of the target site(s) 200.

One of ordinary skill in the art will readily appreciate that the number of images 400, as well as their contents and arrangement may vary, as may the number of images the screen contains. One of ordinary skill in the art will also readily appreciate that notification of the connection between the system 100 and the second party 200 may be provided to the user 10 in a variety of forms, including, but not limited to, by an electronic communication, such as e-mail, or by one or more alternative on-screen notifications. As noted above, the user may view only a single image that is created by the connection to the target site 200.

Once connected to one or more target site(s) 200 through the system 100, the user 10 may continue to browse or navigate through any or all sites anonymously for entertainment or information retrieval purposes. In one embodiment, the user may also engage in electronic commerce transactions through the system 100 with a user-specified level of anonymity or privacy. Generally, the user 10 specifies its desired level of anonymity or privacy to the system by mouse clicking, or otherwise selecting, a hyperlink or message or dialogue box contained within the screen image 400A. It is understood that the user 10 may specify a uniform privacy level for all transactions conducted while connected to the system 100, or may specify differing privacy levels for different transactions. The various privacy level options, which are explained below, range from no anonymity to complete anonymity.

FIG. 7 schematically illustrates a first level privacy transaction between a user 10 and one or more target sites 200 utilizing the intermediary system 100. A first level privacy transaction allows the user to browse Internet sites anonymously, to order items from the sites, and to have purchased items shipped to the user 10 all while maintaining anonymity, including privacy of financial information.

For example, after browsing target site(s) 200 via the system 100 as discussed above, the user 10 may instruct the system 100 to enter a target site 200 that includes a feature allowing it to serve as an electronic commerce vendor site. By accessing a vendor site through, the user 10 can initiate electronic commerce transactions in which goods are purchased on-line. In another embodiment the user places an order for goods through the system. In a further embodiment orders for goods are placed in machine readable form. The system 100 then submits the user's order to the sites (e.g., via the alias identity connection through the system 100). The system 100 transmits to the site or sites 200 transaction purchase instructions. In one embodiment, the transaction purchase instructions in the first level privacy transaction include the user's actual name and address, enabling the target site to ship items directly to the user. Alternatively, the transaction purchase instructions may include an alias for the user and/or a system identifier code for the user, together with at least part of the user's actual address. In yet another embodiment, the transaction purchase instructions include the user's actual or alias identity, a system identifier code for the user, and an address of a third party shipping depot selected by the user (e.g., a post office or a private mailing or shipping facility). The transaction purchase instructions may further include payment instructions, such as authorization to charge the cost of the items purchased to an intermediary system-controlled credit card or to an account maintained by the system with the target site. The transaction purchase instructions may also include shipping instructions, including mode of shipping and identification of a preferred shipping company.

One of ordinary skill in the art will appreciate that transaction purchase instructions can be provided to the vendor by a variety of techniques. For example, these instructions, and payment instructions, can be conveyed to the vendor through an electronic "wallet" software application. The instructions may also be provided to the site(s) 200 by "drag and drop" or "copy and paste" techniques to convey selected information present on the intermediary site to the vendor site. In addition, the desired information can simply be typed by the user.

As the invention is applicable to telephone order and/or mail order transactions, transaction purchase instructions can also be made by voice, by electronic signal (e.g., by telephone touch tone keys), or through mechanical means (e.g., by handwritten instructions).

In one example, the system 100 pays for purchased item(s) with an one of its own credit cards that the target site(s) 200 cannot associate with the user 10. However, the system 100 is able to link the user-assigned system credit card to the user 10 so that the transaction costs can be charged by the system to a user's credit card and/or a user account with the system that was created upon user registration. The system will then, in turn, either debit the user's credit card or the user account for costs associated with the item(s), plus any service charges.

The system will generally possess a plurality of distinct alias credit cards, each of which is preferably unique to each user 10. It is understood, however, that the system 100 may utilize a common alias credit card to pay for item(s) ordered by different users 10. In such an embodiment, these users 10 may be related to each other in some way, such as members of the same company or members of a family, or may be completed unrelated. It is also understood that each alias credit card may be either permanently or temporarily assigned to a user or group of users.

Alternatively, the system payment instructions may simply include a purchase order number which authorizes the target site to charge the purchase price to a preexisting account established by the system with the target site. The purchase order is linked to the user by the system and transaction costs are subsequently billed to the user by the system.

Although not shown in FIG. 7, the present invention may also optionally include an order verification procedure in which the system 100 instructs each target site 200 to hold the user's orders pending final user approval to complete its purchases. In such an embodiment, only after receiving this order verification will the system 100 instruct each target site 200 to process the order.

Once the user's 10 order has been processed and, optionally verified, the transaction continues in accordance with shipping instructions provided to the vendor site 200 by the system 100 simultaneous with or subsequent to transmitting the transaction purchase instructions. In one embodiment, discussed above, the transaction purchase instructions can direct the vendor to ship purchased items using the user's actual name. Although this technique discloses the user's identity to the vendor, it is still effective to preserve the confidentiality of the user's financial and credit information.

FIGS. 8 and 9 depict various embodiments of the invention that utilize a second, higher level of privacy for a transaction between a user 10 and one or more target sites 200 through the system 100. The browsing, ordering, payment and optional order verification portions of these enhanced privacy transactions of FIGS. 8 and 9 are generally identical to the process described above with respect to FIG. 7. To ensure enhanced privacy, the transaction purchase instructions will include shipping instructions that preserve user anonymity. The shipping options can include direct anonymous shipping to the user, and anonymous shipping by the vendor to a site local to the user that is maintained by or affiliated with the system 100. Regardless of the option selected by the user 10, the system's transaction purchase instructions to the vendor will include, as a first component, identifying information for the user, and, as a second component, user location information. The identifying information can be in the form of a user alias name, a code for the user established by the system, or a name, such as a trade name, representative of the system 100. The user location information must normally include the user's actual city/town, state, zip code and, if applicable, country address. The user's street address can be replaced with a specific identifier code, supplied and controlled by the system, that is unique to the user. Alternatively, the user's street address can be replaced with a covert street address information, which may be in the form of a system-generated code for the user that is a party to the transaction.

Thus, in one example, the transaction purchase instructions can be as follows. Where the site 200 requests a "name," the user may provide a name that is indicative or associated with the intermediary host system. Where the site 200 requests a "street address" the user may enter a specific identifier code, supplied by the system, that is unique to the user. The "city/town," "state," and "zip code" fields requested by the site 200 may be filled in using actual information that pertains to the user.

In the embodiment of FIG. 8, once the user's order is processed by the vendor site(s) 200 and, if applicable, verified by the user, the item(s) are packaged and addressed using the user identifying information and the user location information provided by the system. The package is the transferred to a shipping company, which processes it in a typical manner. In the course of processing the package, such a by scanning a bar code or other machine readable label information, the shipping company 500 is able to match user identifying information and user location information with an actual user's name and street address. For example, the shipping company, through a pre-existing relationship with the system 100, will be able to detect embedded, system-generated codes relating to user identity and location, and match the coded information with the user's actual name and street address. In one embodiment, once the coded information is detected and converted to true identity information, the shipping company 500 will automatically generate a new address label containing the user's actual name, street address, city, state and zip code.

The automatic relabelling procedure can take place at a point of transfer to the shipping company (e.g., a Federal Express truck), or it can take place at the shipping company's processing facility. Thus, once the package is identified and attributed to the system, it can be segregated and grouped with other packages attributed to the system. These packages will be subsequently scanned by the shipping company 500 in such a manner that the address code present on each vendor-applied shipping label of each package is detected and matched to its particular system-provided user name. The shipping company 500 then will automatically generate a new address label for each package containing the actual name, street address, city, state and zip code of the user 10 who ordered the package through the system.

One of ordinary skill in the art will readily appreciate that bar code reading and package handling systems currently utilized by shipping companies (e.g., Federal Express, United Parcel Service, etc.) can easily be modified to detect a code that is indicative of a system-related package. Also, data can be exchanged between the system and the shipping company as is generally known in the art in order to enable the shipping company to convert the coded or encrypted address information for a given user into the user's actual address information, and to generate a new shipping label bearing the user's actual address.

It is further understood that there may not be a need for the shipping company to relabel packages. The processing codes (e.g., bar codes) present on the vendor-applied labels may be "two-dimensional." The printed material may include identifying information, such as user alias, that makes it impossible to identify the actual user. However, when the label is scanned by the shipping company, machine readable data identifies the actual user and shipping address and/or instructs the shipping company as to where to deliver the package.

FIG. 9 schematically illustrates another procedure for ensuring an enhanced level of privacy during a transaction. In such an embodiment, once the user's order is processed by the vendor site 200 and, if applicable, verified by the user, the item(s) are packaged and shipped to a predetermined package delivery depot 550 that is local to the user 10. The package delivery depot 550 can be any one of a variety of institutions including, but not limited to, a post office, a private mailing facility (e.g., Mail Boxes Etc.), and a shipping company processing center. The selection of a particular package delivery depot 550 may depend on a number of factors, including, but not limited to, specific user choice or geographic proximity to the user 10.

Generally, the package will be accompanied by either a physical or electronic invoice from the vendor site 200. This invoice contains user identifying information that will allow the package delivery depot 550 to match the package to the user 10 when the user attempts to claim it. The user identifying information may be, for example, the user's name or a user alias, such as the user address code discussed above, or a transaction number assigned by the system 100. It is understood that if the user 10 opts for this particular shipment option, it will have previously notified the system, or will have previously have been notified by the system 100, of the particular user identifying information associated with a particular transaction.

It is further understood that prior to or upon shipment of the item(s) to the package delivery depot 550, the system 100 will inform the user 10 of the location of the package depot to which the package has been sent. The system also will inform the user 10 of the approximate or exact arrival time of the package at the depot 550. The user 10 can thereafter claim the package by providing the depot with the user identifying information.

These enhanced privacy shipment embodiments illustrated in FIGS. 8 and 9 ensure a high level of privacy to the user 10 because although the sites 200 and the vendors associated therewith are aware of exactly what item(s) are being ordered by the user, they do not know the user's identity. Further, while the shipping company 500 (see FIG. 8) or package depot (see FIG. 9) are aware of the name and address of the user 10, it does not know the contents of the package(s) that the user purchased. The confidentiality of the user's financial information is preserved as well.

The present invention also accommodates the delivery of digital goods (e.g., software) from a vendor to a user in an anonymous manner. In this embodiment, the digital goods can be forwarded first to the system and then to the user. Alternatively, the system can transfer, or direct the vendor to transfer, the goods to a secure, system-controlled site on the world wide web and provide the user with a URL link or other means to access the site. Thereafter, the user may access the site and download the digital goods.

As shown in FIG. 10, the system 100 can also be modified to further involve a financial institution 600 in any of the system mediated transactions described above with respect to FIGS. 8 and 9. The financial institution 600 is an authorized third party to the transaction, such as a bank or a credit union. Preferably, the financial institution 600 is one at which the user 10 has funds on account, and/or has a credit account. The involvement of a financial institution can be useful, for example, in the event that the user 10 does not wish to provide the system 100 with credit card and/or financial information, or where the user is unable or does not wish to have transaction costs debited to its credit card.

A transaction in accordance with FIG. 10 generally proceeds identically to any of those described above with respect to FIGS. 7-9, except with respect to the payment portion of the transaction. Once the total costs associated with item(s) purchased from the site(s) 200 have been calculated, the financial institution 600 is requested to provide user funds, or to extend user credit, to cover these costs. This request can come from the user 10, the target site(s) 200, or, preferably, the system 100, and can be made electronically, telephonically, or otherwise as is generally known in the art.

The financial institution 600 then determines whether the user has sufficient funds (or has been extended sufficient credit) to cover the total costs associated with the transaction, including any service charges applied by any party to the transaction. If so, the financial institution 600 either directly remits the funds to the site(s) 200, or remits the funds to the system 100, which, in turn, remits the funds to the site(s). Once each site 200 receives the remitted funds, the process will continue as discussed above with respect to FIGS. 7-9, culminating with the user 10 receiving its ordered item(s) either directly from each site 200 (see FIG. 7), from each site via a shipping company 500 (see FIG. 8), or from each site via a package delivery depot 550 (see FIG. 9).

One of ordinary skill in the art will readily appreciate that the financial institution 600 may require user approval prior to releasing its funds or outlaying its credit in furtherance of each separate transaction. Alternatively, prior to the transaction, the user 10 could authorize the financial institution 600 to outlay a certain amount of user funds or credit to the system 100, such as on a per transaction or per specific time period basis.

Although each of the embodiments of FIGS. 7-10 relate generally to unidirectional identity verification, the system 100 may also mediate a transaction or other type of exchange by requiring that more than one party to the transaction or exchange verify its identity to the system.

For example, two or more parties may contact the system 100 to effectuate a transfer of funds or an exchange of information between them. In either instance, each party transmits identity verification information to the system 100 as discussed above, or as otherwise generally known in the art. This information can be a biometric characteristic sample, a PIN, and/or coded information, each as described above, or other information in lieu of, or in addition to such information. The system 100 will possess or otherwise have access to comparative data to allow it, as discussed above, to verify the identity of each party based on the identity verification information supplied thereby.

One or more parties to the transaction or exchange may also transmit Global Positioning System (GPS) location data to the system 100 in addition to, or in lieu of, any or all of its identity verification information. The GPS data will preferably include GPS time stamp data from a GPS satellite in order to allow the system to verify the physical location of the transmitting party at the time of GPS data transmission.

In an embodiment in which GPS data is provided to the system in addition to other identity verification information, the GPS data is generally encoded in such a manner to ensure relatively contemporaneous acquisition of the party's GPS data and the its identity verification information. This may be done, for example, by co-encrypting the party's GPS data with a component of the party's identity verification information as is generally known in the art.

Once the requisite identity verification information and/or GPS data of some or all of the parties is received by the system 100, the system compares the information with the comparative data of each party. If the information matches this comparative data exactly or to an allowable degree, the system 100 then alerts each party to this fact, and the parties may then conduct their desired transaction or exchange.

In addition to the parties noted above with respect to FIGS. 7-10, this type of identity verification procedure may be used by any party that desires some level of identity verification from another party before exchanging information and/or conducting a transaction with that party. Exemplary such additional parties include, but are not limited to, financial institutions, hospitals, research laboratories, and governments and their bureaus or agencies.

Referring now to FIGS. 11 and 12, the user 10 may also utilize the intermediary system 100 to facilitate the return or exchange of items purchased in accordance with the embodiments of FIGS. 7-10 while retaining a desired degree of privacy and anonymity. To initiate a return or exchange, the user 10 logs into the system 100 in the manner described above and enters (e.g., clicks on a hyperlink) a return loci, an area of the system dedicated to handling returns and exchanges. The return loci prompts the user 10 to provide the system with data that allows the system 100 to recall information for the specific transaction to which the return or exchange relates. This information may include, for example, the site(s) from which the item(s) were purchased, the transaction number, the user alias for the transaction, and/or the shipping address code used for the transaction.

The system 100 then contacts each relevant site 200, and requests authorization for the return or exchange. Once each site 200 authorizes the return or exchange, the user 10 can return the item(s) to each site in any manner desired. As noted above, however, the user 10 will generally wish to do so in such a manner as to preserve its anonymity, while also ensuring that the purchase price is credited to its account with the system 100, or that suitable replacement merchandise will be received.

FIG. 12 depicts exemplary return processes designed to preserve user 10 anonymity. Once the user 10 receives authorization for a return or exchange, it sends each item either to the system 100, or to the site 200 from which each item was purchased. In each instance, the user 10 sufficiently indicates whether the items are being returned for a refund, exchanged for another item, or returned for replacement with an identical item.

If the user 10 returns each item to the system 100, the system may immediately credit the user's credit card or system account for the cost of the item. The system 100 then sends the item(s) to the appropriate site(s) 200, replacing the user's 10 identity and address information with information consistent with the alias (including name and/or shipping address) under which the merchandise was originally purchased.

Alternatively, the user 10 may return items directly to the appropriate site(s) 200 from which they were ordered. To do so, the user 10 must first obtain applicable code information from the system 100. This code information may include the alias name and/or coded address under which the purchase was originally made. This coded information can be automated in such a way that, upon request or instructions made at the return loci of the system 100, the user 10 can direct the appropriate return label(s) and/or form(s) to be printed on a printer local to the user. These labels and forms would then be used to ship the return package directly to the site(s) 200 from which they were ordered, while preserving user 10 anonymity.

One of ordinary skill in the art will appreciate that in the event of a return or exchange, a variety of scenarios can be effected to ensure that all parties to the transaction, and the intermediary system 100 are provided with the finds and/or merchandise they deserve. For example, a refund will require that the site(s) 200, in exchange for the returned item(s), credit the account used to purchase the item(s). Depending upon the payment option utilized bu the user 10 and the system 100, the cost incurred by the user and system should be a net zero.

Referring now to FIGS. 13-15, in any transaction involving the system 100, the user 10, one or more second parties 200 and an authorized third party 600 (e.g., a financial institution such as a bank or credit union), the split image 400 embodiment of the present invention (as depicted in FIG. 6, and as described above) may be further and/or differently split as shown in FIGS. 13-15 to reflect the connections between any or all of the these parties during such a transaction.

In such an embodiment, a portion (700A in FIG. 13, 800A in FIG. 14, 900A in FIG. 15) of the image (700 in FIG. 13, 800 in FIG. 14, 900 in FIG. 15) will generally display the connection between the user 10 and the site(s) 200, and a portion (700B in FIG. 13, 800B in FIG. 14, 900B in FIG. 15) of the image generally will display the connection between the system 100 and the site(s).

Each of the displayed images 700, 800, 900 of FIGS. 13-15 may also display at least one additional connection. For example, as shown in FIG. 13, a portion 700C of the image 700 may additionally display the connection between the system 100 and the financial institution 600. Also, as shown in FIG. 14, a portion 800C of the image 800 may additionally display the connection between the user 10 and the financial institution 600. And, as shown in FIG. 15, the screen 900 may additionally display the connection between the system 100 and the financial institution 600 as well as the connection between the user 10 and the financial institution. Each of the portions (700A-C, 800A-C, 900A-D) of the images 700, 800, 900 of FIGS. 13-15 are updated during the various stages of a transaction in accordance with the present invention.

Any connection that is not between the user 10 and another party will generally be displayed in the form of a clone, as described above. Also, one of ordinary skill in the art will readily appreciate that the number, arrangement, and contents of the screens 700, 800, 900 of FIGS. 13-15 may vary.

One of ordinary skill in the art will appreciate that the intermediary system can be virtually any entity. In one embodiment, the intermediary is a private independent entity. The intermediary may, however, be an entity that is affiliated or associated with another organization such as a shipping company, a financial institution, or a vendor.

One of ordinary skill in the art will readily appreciate that, in a transaction involving the intermediary system, a first party or user(e.g., a consumer), one or more second parties (e.g., one or more vendors), and one or more optional authorized third party (e.g., a financial institution and/or a shipping company), any or all of the parties can interact in ways in lieu of, in addition to any or all of those described above in furtherance of a transaction occurring on a communication network. Thus, one skilled in the art will also appreciate further features and advantages of the invention based on the above-described embodiments. Accordingly, the invention is not to be limited by what has been particularly shown and described, except as indicated by the appended claims. All publications and references cited herein are expressly incorporated herein by reference in their entirety.

What is claimed is:

1. A method for facilitating anonymous transactions over a communications network, comprising:

enabling a user to access an intermediary host site through the communications network;

delivering an instruction over the communications network, from the user to the intermediary host site, causing the intermediary host site to form a connection on the communications network between the intermediary host site and a desired vendor site present on the communications network;

granting the user access to the desired vendor site through the connection maintained between the intermediary host side and the desired vendor site, without the vendor site detecting the identity of the user on the vendor site; and

enabling the user to purchase or more items from the vendor site without the vendor site ascertaining the identity of the user.

2. The method of claim 1, wherein the step of enabling the user to access the intermediary host site is conditioned upon the user providing identity verification data to the intermediary host site.

3. The method of claim 2, wherein the identity verification data necessary to access the intermediary host is provided by the user to the intermediary by a registration process.

4. The method of claim 3, wherein the registration process is a multi-step registration process.

5. The method of claim 4, wherein during a first step of the multi-step registration process the user supplies to the intermediary data selected from the group consisting of personal information; financial information; credit information; and combinations thereof.

6. The method of claim 5, wherein the personal information includes information selected from the group consisting of name, address, birth date, social security number, family information, and combinations thereof.

7. The method of claim 6, wherein the financial information includes bank account numbers.

8. The method of claim 7, wherein the credit information includes information selected from the group consisting of one or more debit card account numbers, one or more credit card account numbers, credit card expiration dates, and combinations thereof.

9. The method of claim 4, wherein during a second step of the multi-step registration process the intermediary provides the user with a user ID card that has linked thereto a personal identification number (PIN).

10. The method of claim 9, wherein the PIN provided by the intermediary is temporary and is selectively changeable by the user.

11. The method of claim 4, wherein a third step of the multi-step registration process requires the user to submit to the intermediary a biometric characteristic standard unique to the user.

12. The method of claim 11, wherein the biometric characteristic standard is selected from the group consisting of ocular-based identification characteristics, manual-based, identification characteristics, pedal-based identification characteristics, a voice pattern, a handwriting sample, a stroke pattern, and combinations thereof.

13. The method of claim 12, wherein the ocular-based identification characteristics are selected from the group consisting of a partial retinal scan; a complete retinal scan; an iris scan; and combinations thereof.

14. The method of claim 2, wherein the step of the user providing verification data requires providing two levels of authenticating data.

15. The method of claim 14, wherein the two levels of authenticating data include a first level selected from the group consisting of a code displayed on an user ID card, a code embedded in an ID card in a machine readable form, and combinations thereof, and a second level represented by a personal identification number (PIN) known to the user.

16. The method of claim 15, wherein the code is selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

17. The method of claim 16 wherein the intermediary is equipped with a master code reader that is able to perceive the correct code of the ID card of each user at any point in time.

18. The method of claim 15, wherein the code is present in a chip that produces time variable code selected from the group consisting of an alphabet-based code; a numeric code; and an alphanumeric code unique to the user.

19. The method of claim 15, wherein the code in machine readable form is selected from the group consisting of a bar code, a magnetic strip, and an RF chip.

20. The method of claim 2, wherein the step of the user providing verification data requires providing three levels of authenticating data.

21. The method of claim 20, wherein the three levels of authenticating data include a first level selected from the group consisting of a code displayed on an ID card, a code embedded in an ID card in a machine readable form, and combinations thereof, a second level in the form of a personal identification number (PIN) known to the user, and a third level in the form of a biometric characteristic unique to the user.

22. The method of claim 21, wherein the code is selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

23. The method of claim 21, wherein the code is present in a chip that produces a time variable code selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

24. The method of claim 21, wherein the code in machine readable form is selected from the group consisting of a bar code, a magnetic strip, and an RF chip.

25. The method of claim 21, wherein the biometric characteristic unique to the user is selected from the group consisting of ocular-based identification characteristics, manual-based identification characteristics, pedal-based identification characteristics, a voice pattern, a handwriting sample, a stroke pattern, and combinations thereof.

26. The method of claim 25, wherein the ocular-based identification characteristics are selected from the group consisting of a partial retinal scan; a complete retinal scan; an iris scan; and combinations thereof.

27. The method of claim 25, wherein the biometric characteristics of the user are sampled, prior to the user gaining access to the intermediary host site, through a device that is connected to the communications network and local to the user.

28. The method of claim 1, wherein the communications network is the Internet and the step of enabling the user to access the intermediary host site is conditioned upon the user providing identity verification data to the intermediary host site.

29. The method of claim 28, wherein the step of enabling the user to access the intermediary host site is conditioned upon the user providing identity verification data to the intermediary host site.

30. The method of claim 29, wherein the at least one second party is any entity having an Internet protocol (IP) address on the world wide web.

31. The method of claim 30, wherein a request by the user for the intermediary host site to connect to a specified Internet Protocol (IP) address causes the intermediary host site to effect a connection with the specified IP address using identifying data packets that are indicative of the intermediary host site, and grant the user access to the connection.

32. The method of claim 31, wherein the connection to which the user has been granted access by the intermediary host site is displayed on a user computer monitor.

33. The method of claim 32, wherein http calls made by the user are relayed to the specified IP address by the host intermediary site.

34. The method of claim 33, wherein the user computer monitor displays a split image in which a first image displays an image of the specified IP address and a second image displays an image representative of the intermediary host site.

35. A method for facilitating anonymous electronic transactions on the world wide web between a user and at least one vendor site on the world wide web, comprising:

providing an intermediary host site having an Internet Protocol (IP) address on the world wide web, which may be accessed by a user;

enabling the user to access an intermediary host site through the world wide web;

delivering an instruction over the world wide web, from the user to the intermediary host site, causing the intermediary host site to form a connection on the world wide web with a desired vendor site having an IP address on the world wide web;

granting the user access to the desired vendor site through the connection maintained between the intermediary host site and the desired vendor site, without the vendor site detecting the identity of the user; and enabling the user to purchase one or more items from the vendor site without the vendor site ascertaining the identity of the user..

36. The method of claim 35, wherein the user is able to access the intermediary host site through an Internet portal.

37. The method of claim 36, wherein multiple users are able to access the intermediary host site.

38. The method of claim 37, wherein any user of a group of multiple users is able to, sequentially, instruct the intermediary host site to form a connection to multiple desired vendor sites and access the multiple vendor sites without any one of the multiple vendor sites detecting the identity of the user or the presence of the user on the desired vendor site.

39. The method of claim 38, wherein the step of enabling a user to access the intermediary host site is conditioned upon the user providing identity verification data to the intermediary host site.

40. The method of claim 39, wherein the step of the user providing identity verification data requires providing two levels of authenticating data.

41. The method of claim 40, wherein the two levels of authenticating data include a first level selected from the group consisting of a code displayed on an ID card, a code embedded in an ID card in a machine readable form, and combinations thereof, and a second level in the form of a personal identification number (PIN) known to the user.

42. The method of claim 41, wherein the code is selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

43. The method of claim 41, wherein the code is present in a chip that produces a time variable code selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

44. The method of claim 43, wherein the code in machine readable form is selected from the group consisting of a bar code, a magnetic strip, and an RF chip.

45. The method of claim 39, wherein the step of the user providing verification data requires providing three levels of authenticating data.

46. The method of claim 45 wherein the three levels of authenticating data include a first level selected from the group consisting of a code displayed on an ID card, a code embedded in an ID card in a machine readable form, and combinations thereof, a second level in the form of a personal identification number (PIN) known to the user, and a third level in the form of a biometric characteristic unique to the user.

47. The method of claim 46, wherein the code is selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

48. The method of claim 47, wherein the code is present in a chip that produces a time variable code selected from the group consisting of an alphabet-based code, a numeric code, and an alphanumeric code unique to the user.

49. The method of claim 47, wherein the code in machine readable form is selected from the group consisting of a bar code, a magnetic strip, and an RF chip.

50. The method of claim 45, wherein the biometric characteristic unique to the user is selected from the group consisting of ocular-based identification characteristics, manual-based identification characteristics, pedal-based identification characteristics, a voice pattern, a handwriting sample, a stroke pattern, and combinations thereof.

51. The method of claim 50, wherein the ocular-based identification characteristics are selected from the group consisting of a partial retinal scan, a complete retinal scan, an iris scan, and combinations thereof.

52. The method of claim 51, wherein the intermediary is equipped with a master code reader that is able to perceive the correct code of the user ID card of each user at any point in time.

53. The method of claim 43, wherein the biometric characteristics of the user are sampled prior to the user gaining access to the intermediary host site.

54. The method of claim 39, wherein the step of granting the user access to the desired vendor site further comprises causing the intermediary host site to create a clone image of a computer monitor-displayed image of the desired vendor site and causing the intermediary host site to grant the user access to the clone image.

55. The method of claim 54, wherein the clone image to which the user has been granted access by the intermediary host site is displayed on a user computer monitor.

56. The method of claim 55, wherein http calls made by the user to the clone image of the desired vendor site are relayed to the desired vendor site by the host intermediary site through the connection to the desired vendor site that is maintained between the alias identity and the intermediary host site.

57. The method of claim 56, wherein the user computer monitor displays a split image in which a first image displays the clone image and second image displays an image of at least one page linked to the intermediary host site IP address.

58. The method of claim 39, wherein the step of enabling a user to purchase further comprises the steps of:

enabling the user to complete a transaction, through the intermediary host site, in which the user purchases at least one item from at least one desired vendor site, the transaction occurring with a desired level of privacy; and

the user transmitting to the at least one desired vendor site a set of user transaction purchase instructions.

59. The method of claim 58, wherein the transaction purchase instructions include alias identity information selected from the group consisting of an actual name for the user, an alias name for the user, an intermediary host site identifier code for the user, an actual street address for the user, a fictitious street address for the user, a system-controlled code unique to the user, a shipping address for a facility affiliated with the intermediary host site, an actual city/town, state and zip code for the user, and combinations thereof.

60. The method of claim 59, wherein the alias name for the user is a name indicative of the intermediary host site.

61. The method of claim 59, wherein the transaction purchase instructions further includes payment instructions.

62. The method of claim 61 wherein the user, following or simultaneous with the step of completing a transaction, issues form-of-payment instructions to the intermediary host site.

63. The method of claim 62, wherein the form-of-payment instructions include authorization to charge the cost of the transaction to a credit account or a debit account of the user.

64. The method of claim 63, wherein the credit account is one or more credit cards issued to the user.

65. The method of claim 63, wherein upon receiving the form-of-payment instructions issued by the user, the intermediary host site assigns an intermediary-controlled credit card to the user for at least the transaction and authorizes the desired vendor site to charge the cost of the at least one item to the intermediary-controlled credit card.

66. The method of claim 65, wherein the transaction purchase instructions further include shipping instructions, including mode of shipment and a shipping company identity.

67. The method of claim 66, wherein the shipping instructions further include information selected from the group consisting of the user's actual address, a third party shipping depot address, and a fictitious shipping address having at least a first component and a second component.

68. The method of claim 67, wherein the first component of the fictitious shipping address includes one or more items selected from the group consisting of an alias name for the user, a intermediary-controlled address code for the user, an intermediary-controlled code for the transaction, a name indicative of the intermediary host site, and combinations thereof.

69. The method of claim 68, wherein the second component of the fictitious shipping address includes the actual city/town, state and zip code address of the user.

70. The method of claim 69, wherein upon transmittal by the desired vendor site of a package containing the at least one item that is the subject of the transaction, the shipping company identified in the mode of shipment instructions processes the package independent of the desired vendor site to deliver it to the user by taking an action selected from the group consisting of: delivering the package to the actual user address noted on a shipping label affixed to the package; detecting the intermediary-controlled address code unique to the actual user, via data provided by the intermediary host site, relabelling the package with a shipping label bearing the user's actual address and

delivering the relabelled package to the actual user; detecting the intermediary-controlled address code unique to the actual user, via data provided by the intermediary host site, determining the user actual identity and address based on the code and delivering the package to the user; and delivering the package to the third party shipping depot address displayed on a shipping label affixed to the package.

71. The method of claim 58 wherein the intermediary host site is maintained by a shipping company.

72. A method for facilitating and implementing privacy in an electronic transaction, comprising:

providing an intermediary host site having a site on the Internet;

registering at least one system user as an authorized member of the intermediary host site;

enabling at least one system user to access the intermediary host site through the Internet upon the at least one system user providing identity verification data to the intermediary host site sufficient to establish that the at least one system user is the authorized member that the at least one system user purports to be;

enabling the at least one system user to transmit instructions to the intermediary host site over the Internet, requesting the intermediary host site to access a desired vendor site on the Internet;

establishing an Internet connection between the intermediary host site between the desired vendor site;

granting the at least one system user electronic and visual access to the connection between the intermediary host site and the desired vendor site without the desired vendor site detecting the identity of the at least one system user or on the desired vendor site; and

enabling the at least one system user to purchase one or more items from the desired vendor site through the Internet connection by the intermediary host site and the desired vendor site, without the desired vendor site detecting the identity of the at least one system user on the desired vendor site.

73. The method of claim 72, wherein the step of enabling the at least one system user to purchase further comprises the steps of:

the at least one system user completing a transaction in which the at least one user purchases at least one item from the desired vendor site; and

transmitting user transaction purchase instructions to the desired vendor site.

74. The method of claim 73, wherein the at least one system user is able to access and transact with multiple desired vendor sites.

75. The method of claim 73, wherein the transaction purchase instructions include information selected from the group consisting of an actual name for the user, an alias name for the system user, an intermediary host site identifier code for the system user, a system-controlled code unique to the user, an actual street address for the system user, a fictitious street address for the system user, a shipping address for a facility affiliated with the intermediary host site, an actual city/town, state and zip code for the system user, and combinations thereof.

76. The method of claim 75, wherein the alias name for the system user is a name indicative of the system.

77. The method of claim 75, wherein the transaction purchase instructions further include payment instructions.

78. The method of claim 77 wherein the system user, following or simultaneous with the step of completing a transaction, issues form-of-payment instructions to the intermediary host site.

79. The method of claim 78, wherein the form-of-payment instructions include authorization to charge the cost of the transaction to a credit account or a debit account of the user.

80. The method of claim 79, wherein the credit account is one or more credit cards issued to the system user.

81. The method of claim 80, wherein upon receiving form-of-payment instructions from the system user, the intermediary host site assigns an intermediary-controlled credit card to the system user for the transaction and authorizes the desired vendor site to charge the cost of the at least one item to the intermediary-controlled credit card.

82. The method of claim 81, wherein the transaction purchase instructions further include shipping instructions, including mode of shipment.

83. The method of claim 82, wherein the shipping instructions further include information selected from the group consisting of the system user's actual address, a third party shipping depot address, and a fictitious shipping address having at least a first component and a second component.

84. The method of claim 82, wherein the first component of the fictitious shipping address includes items selected from the group consisting of an alias name for the system user, a intermediary-controlled address code for the system user, an intermediary-controlled code for the transaction, a name indicative of the intermediary host site, and combinations thereof.

85. The method of claim 84, wherein the second component of the fictitious shipping address includes the actual city/town, state and zip code address of the user.

86. The method of claim 85, wherein upon transmittal by the desired vendor site of a package containing the at least one item that is the subject of the transaction, the shipping company identified in the mode of shipment instructions processes the package independent of the desired vendor site to deliver it to the system user by taking an action selected from the group consisting of: delivering the package to the actual system user address noted on a shipping label affixed to the package; detecting the intermediary-controlled address code unique to the actual system user, via data

provided by the intermediary host site, relabelling the package with a shipping label bearing the system user's actual address and delivering the relabelled package to the actual system user; detecting the intermediary-controlled address code unique to the actual user, via data provided by the intermediary host site, determining the user actual identity and address based on the code and delivering the package to the user; and delivering the package to the third party shipping depot address displayed on a shipping label affixed to the package.

87. The method of claim 86, wherein the identity verification requires at least two levels of identity authentication.

88. The method of claim 87, wherein the identity verification requires a third level of identity authentication.

89. The method of claim 87, wherein the visual access of the at least one system user to the connection is displayed as an image on a user computer monitor.

90. The method of claim 89, wherein the image is a split image having a first component representing an image of the Internet connection by the intermediary host site between the alias identity and the desired vendor site, and a second component representing an image of the Internet connection between the at least one system user and the intermediary host site.

91. The method of claim 73, where in the intermediary host site is maintained by a shipping company.

92. A method for anonymously acquiring items from a vendor, comprising:

placing an order to purchase goods from the vendor using an alias name;

providing shipping instructions to the vendor, including the mode of shipment, purchaser actual city, state and postal code, and a code representative of the purchaser's actual desired shipment address, wherein the purchaser's actual, desired shipment address is not discernible by the vendor;

causing a third party carrier to have information necessary to ascertain the purchaser's actual desired shipment address based on the code; and

causing the goods to be transferred to the third party carrier for distribution to the purchaser at the actual, desired shipment address; and

causing the third party carrier to ascertain the purchaser's actual desired shipment address from the code, and to ship the goods to the desired shipment address.

93. The method of claim 92, wherein the actual, desired shipment address is a residential or business address of the purchaser.

94. The method of claim 93, wherein the actual, desired shipment address is an address of a shipping depot.

95. The method of claim 94, wherein the shipping depot is selected from the group consisting of a post office, a private mailing facility, and a package distribution and shipping facility.

96. A method of preserving purchaser anonymity in on-line purchasing transactions, comprising:

enabling a purchaser to anonymously access one or more Internet sites maintained by one or more vendors;

enabling the purchaser to purchase goods from the vendor by providing purchase instructions to the vendor, wherein the purchase instructions include an actual city, state, and postal code for the shipment destination and a code representative of the shipment destination and mode of shipment instructions;

allowing the goods to be transferred from the vendor to a shipping company identified in the mode of shipment instructions;

enabling the shipping company to discern an actual shipment destination for the purchaser based upon the code representative of the shipment destination; and

causing the goods to be shipped to the actual shipment destination for the purchaser without the vendor having knowledge of the purchaser's identity or actual address.

97. The method of claim 96, wherein the code representative of the shipment destination is in machine readable form and wherein the shipping company is able to interpret the code to determine the actual shipment destination.

98. The method of claim 97, wherein the actual shipment destination is a residential or business address of the purchaser.

99. The method of claim 97, wherein the actual shipment destination is an address of a shipping depot.

100. The method of claim 99, wherein the shipping depot is selected from the group consisting of a post office, a private mailing facility, and a package distribution and shipping facility.

101. The method of claim 97, wherein the shipping company serves as a transaction intermediary by enabling the purchaser to anonymously access vendor sites and facilitate the anonymous purchase of goods.

102. A method for facilitating anonymous electronic transactions on the world wide web between a user and at least one vendor site on the world wide web, comprising:

providing an intermediary host site having an Internet Protocol (IP) address on the world wide web, which may be accessed by a user;

enabling the user to access an intermediary host site through the world wide web;

delivering an instruction over the world wide web, from the user to the intermediary host site, causing the intermediary host site to form a connection on the world wide web with a desired vendor site having an IP address on the world wide web;

granting the user access to the desired vendor site through the world wide web connection maintained between the intermediary host site and the desired vendor site through the world wide web;

enabling the user to purchase one or more items from the vendor site; and

enabling the user to issue payment instructions to the vendor site that require purchase charges to be made to an intermediary host-controlled account without revealing user financial information to the vendor site.

103. The method of claim 102, wherein the intermediary host-controlled account is a credit card issued to the intermediary host site and at least temporarily assigned by the intermediary host site to a given user.

104. The method of claim 103, wherein the intermediary host site has a plurality of user-assignable credit cards, each of which may be assigned to at least one user to facilitate the at least one user issuing purchase instructions to the vendor site to enable purchases to be made from the vendor site by the at least one user.

105. The method of claim 102, wherein the intermediary host-controlled account is a preexisting charge account established by the intermediary host site with the vendor site.

106. The method of claim 105, wherein the purchase instructions further include a purchase order number authorizing the cost of goods to be charged to the intermediary host-controlled account.

107. The method of claim 102, further comprising the step of the intermediary host site processing purchase charges made by the user to the intermediary host-controlled account and charging the costs to a user account, in a manner that cannot be perceived by the vendor site.

108. The method of claim 107, wherein the user account is a credit card.

109. The method of claim 107, wherein the user account is a credit account established by the user with the intermediary host site.

110. The method of claim 102, wherein the user does not reveal its true identity to the vendor site during the purchase of goods or through the issuance of the purchase instructions.

111. The method of claim 102, wherein the user is able to access the desired vendor site through the world wide web connection without the vendor site detecting the true identity of the user.

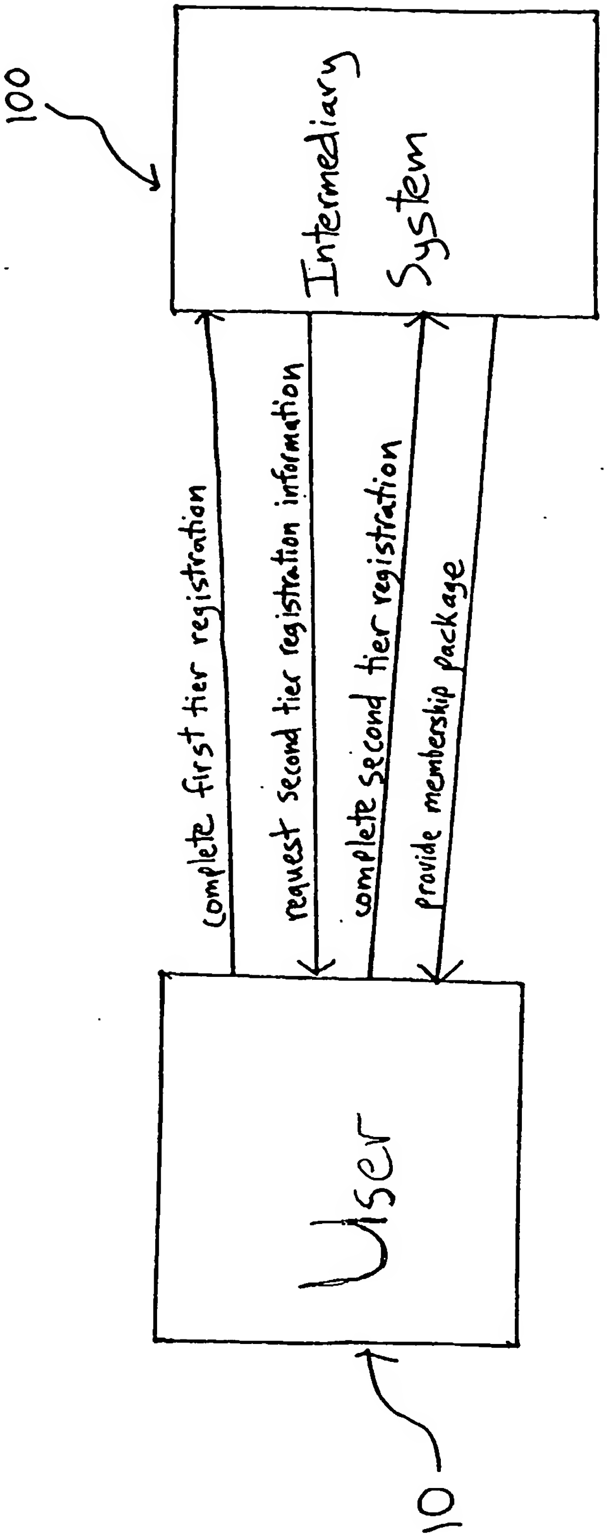

100
Intermediary System
complete first tier registration
request second tier registration information
complete second tier registration
provide membership package
User
10

FIG. 1

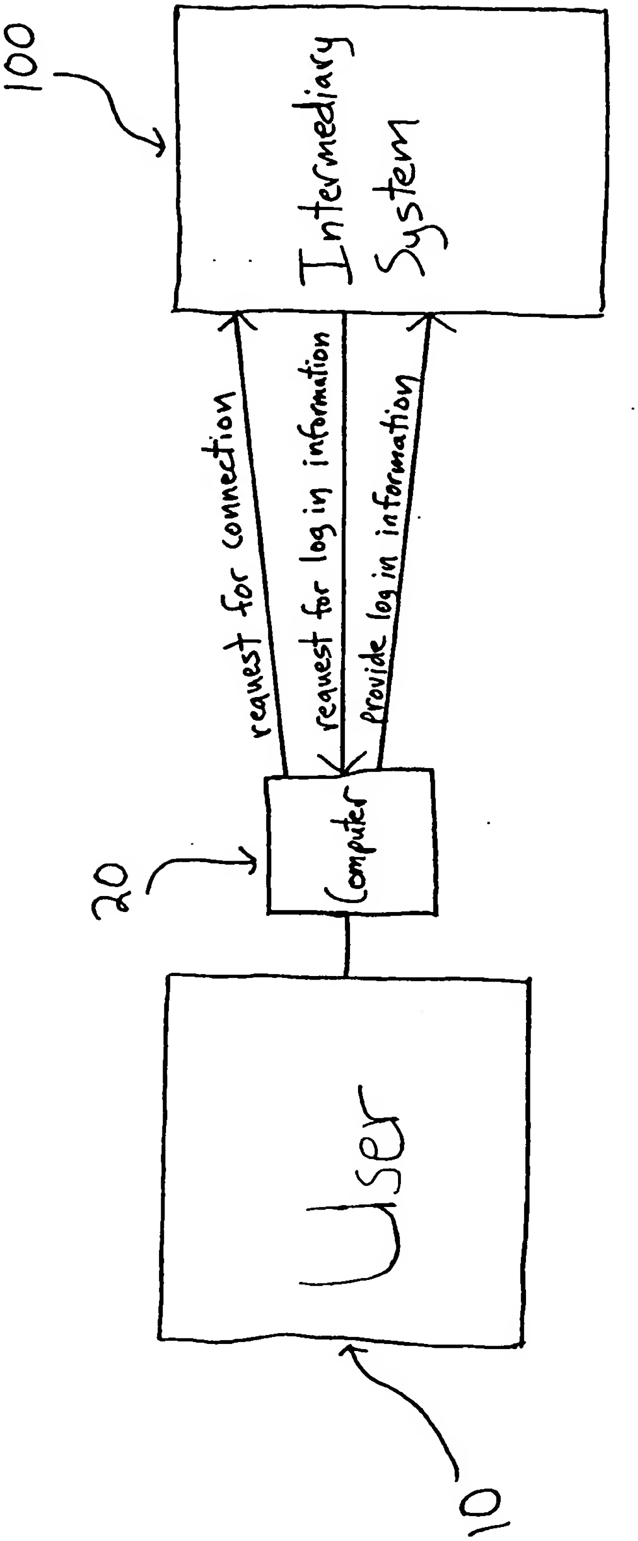

100
Intermediary System
request for connection
request for log in information
Provide log in information
20
Computer
User
10

FIG. 2

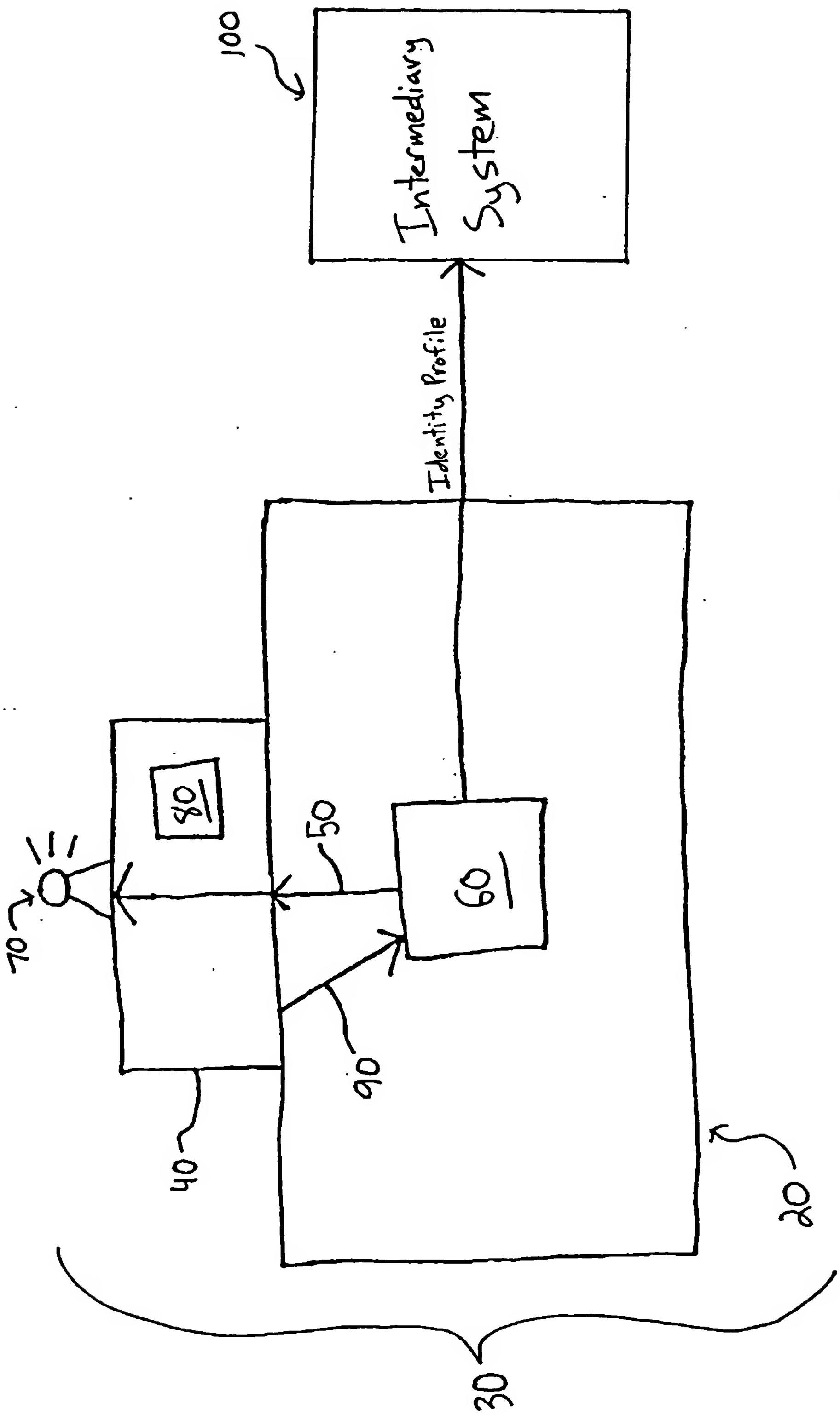

100
Intermediary System
Identity Profile
70
80
50
60
90
40
20
30

FIG. 3

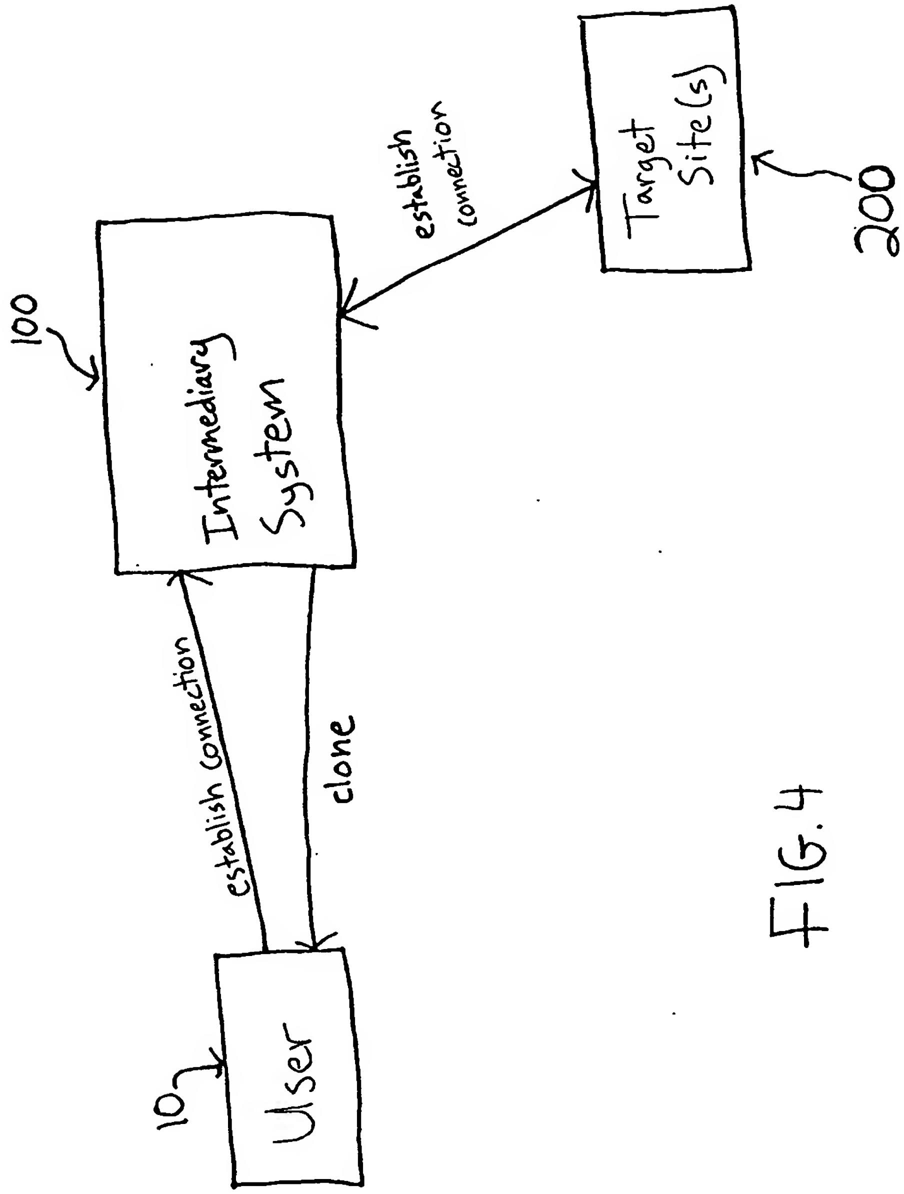

Target Site(s)
200
establish connection
Intermediary System
100
establish connection
clone
User
10

FIG.4

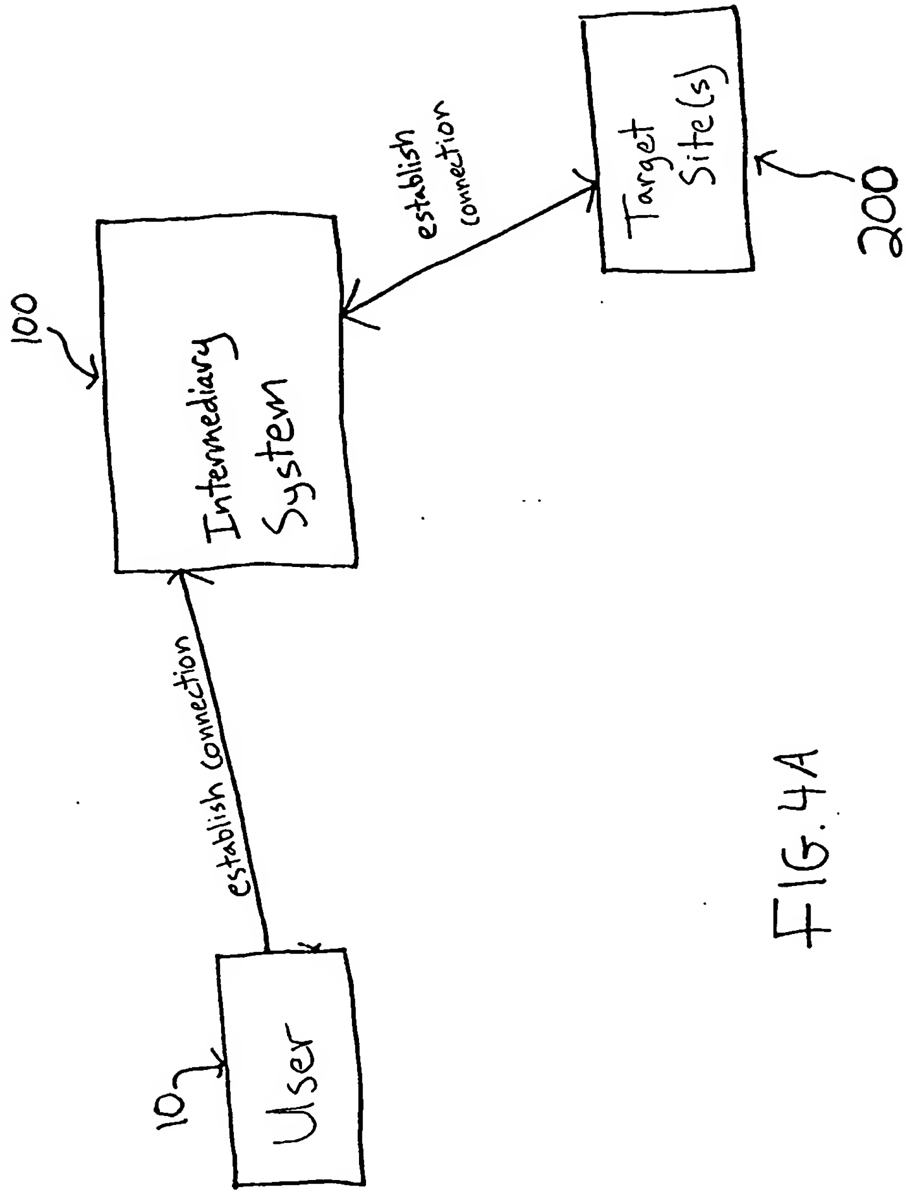

100
Intermediary System
establish connection
Target Site(s)
200
establish connection
User
10

FIG. 4A

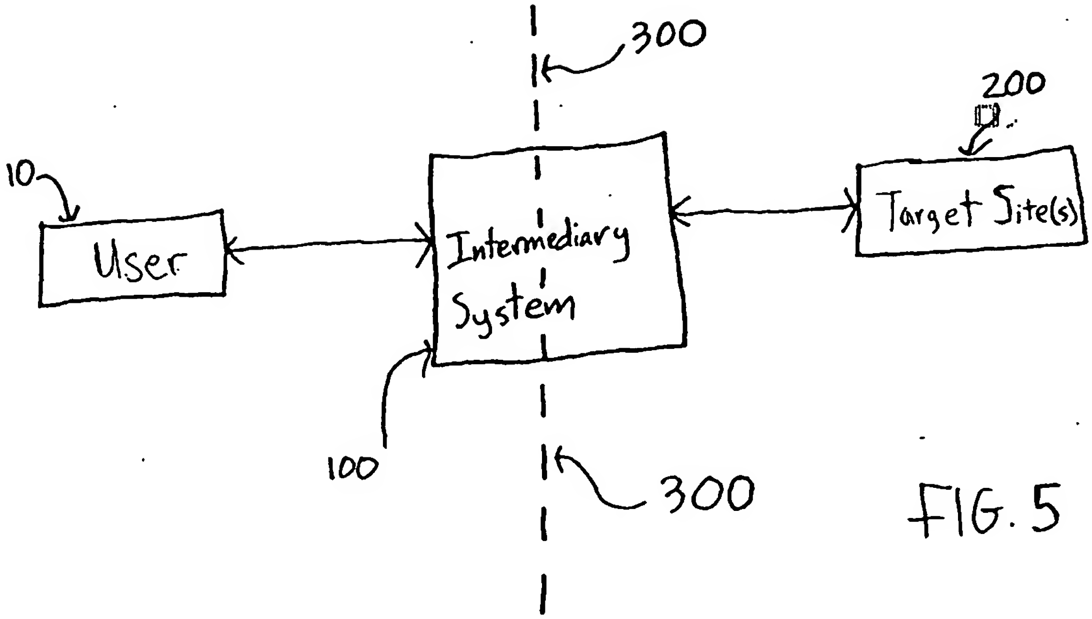

300
200
10
User
Intermediary System
Target Site(s)
100
300

FIG. 5

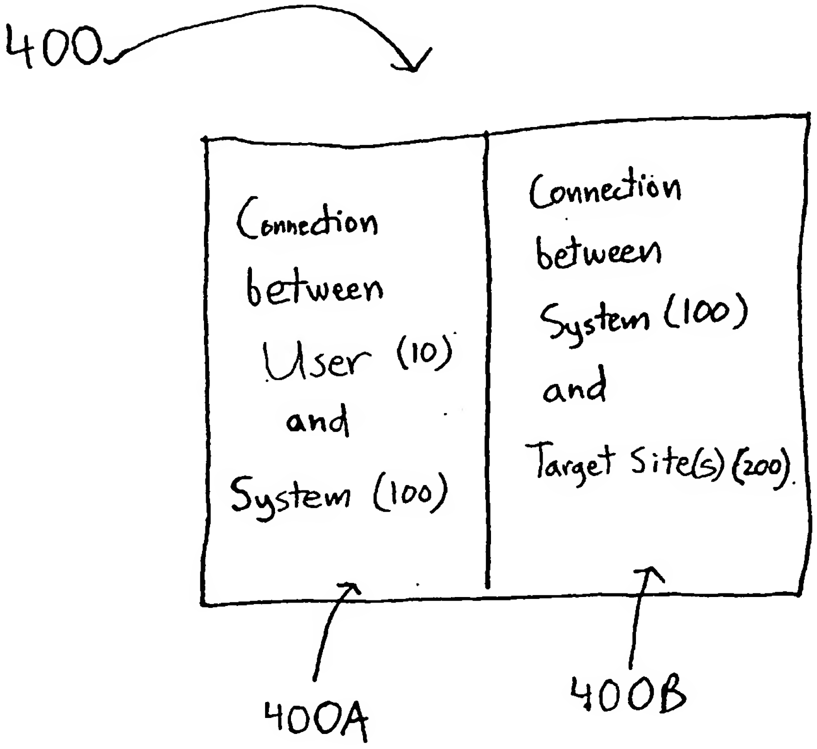

400
Connection between User (10) and System (100)
Connection between System (100) and Target Site(s) (200)
400A
400B

FIG. 6

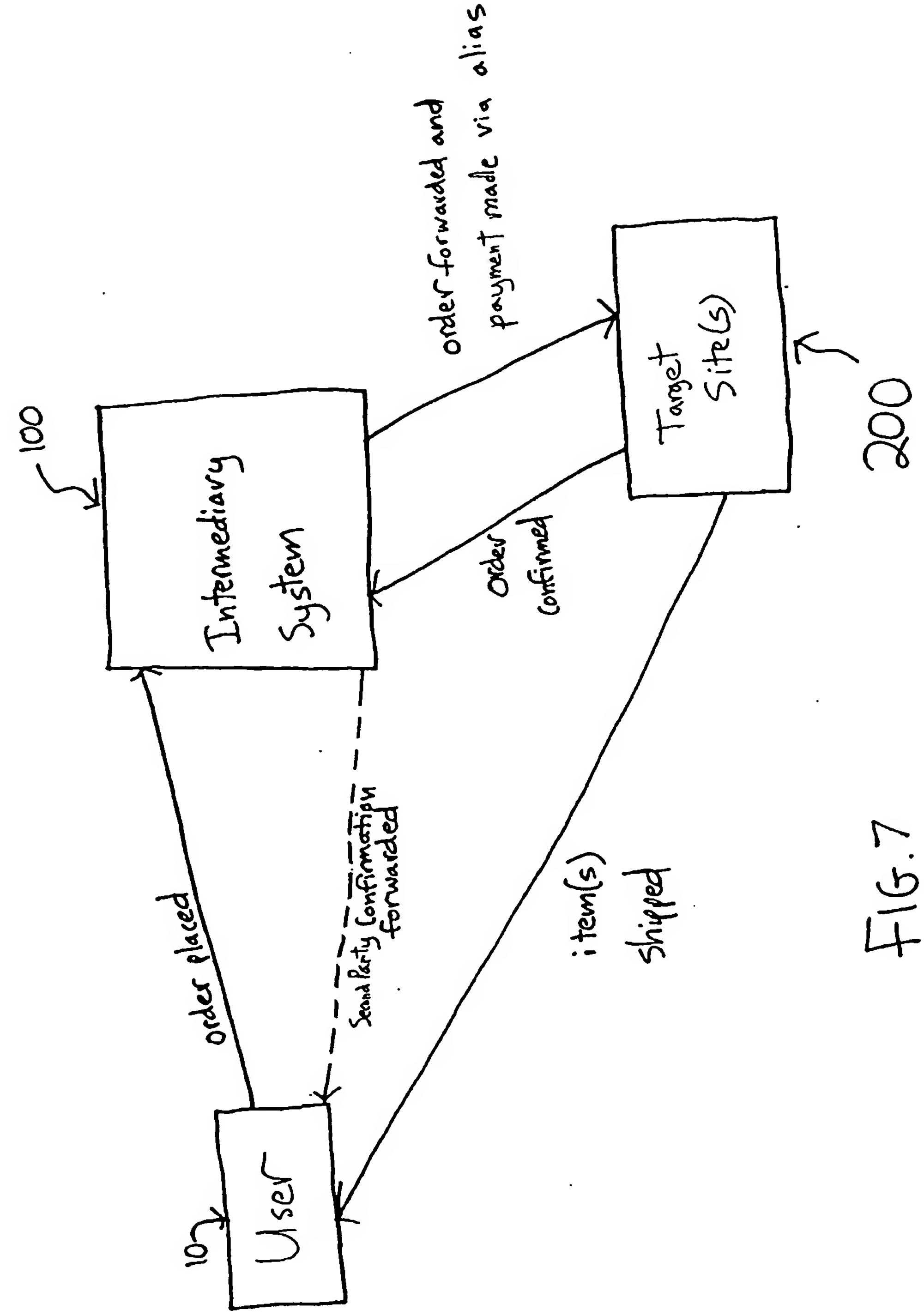

100
Intermediary System
order forwarded and payment made via alias
Target Site(s)
200
order confirmed
order placed
Second Party Confirmation forwarded
item(s) shipped
10
User

FIG.7

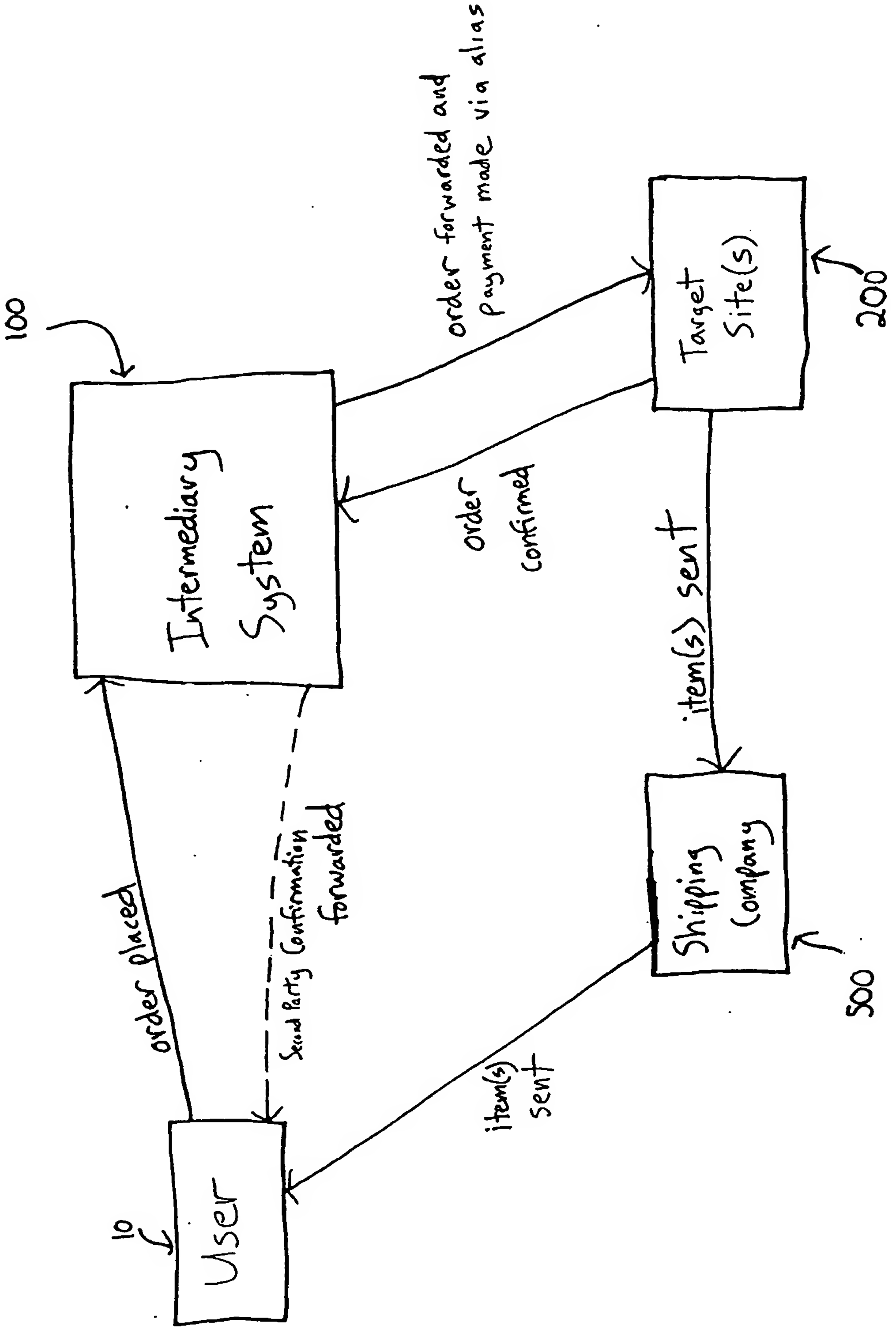

100
Intermediary System
order forwarded and payment made via alias
order confirmed
Target Site(s)
200
item(s) sent
Shipping Company
500
order placed
Second Party Confirmation forwarded
item(s) sent
10
User

FIG. 8

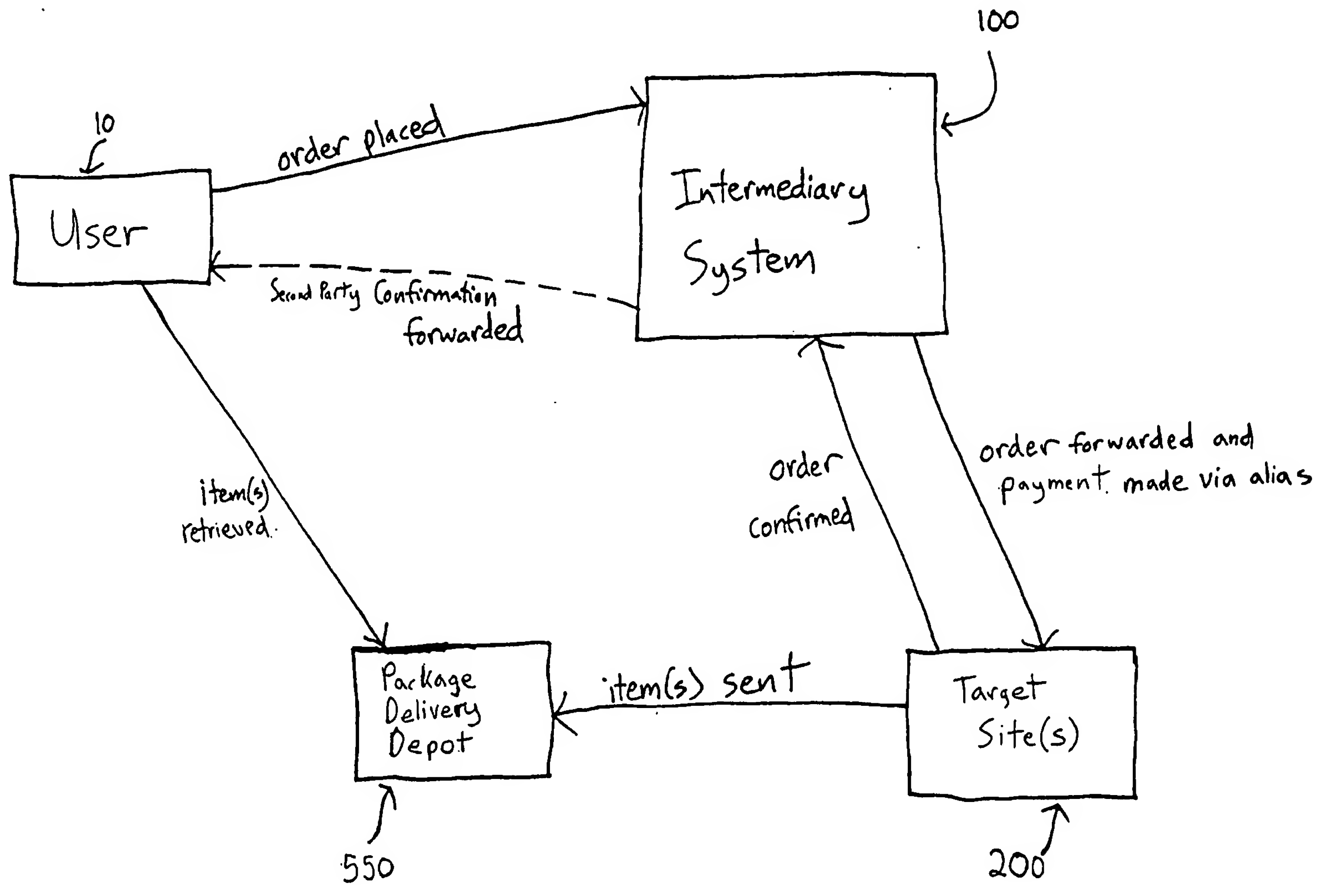

10
User
order placed
100
Intermediary System
Second Party Confirmation forwarded
item(s) retrieved
order confirmed
order forwarded and payment made via alias
Package Delivery Depot
item(s) sent
Target Site(s)
550
200

FIG.9

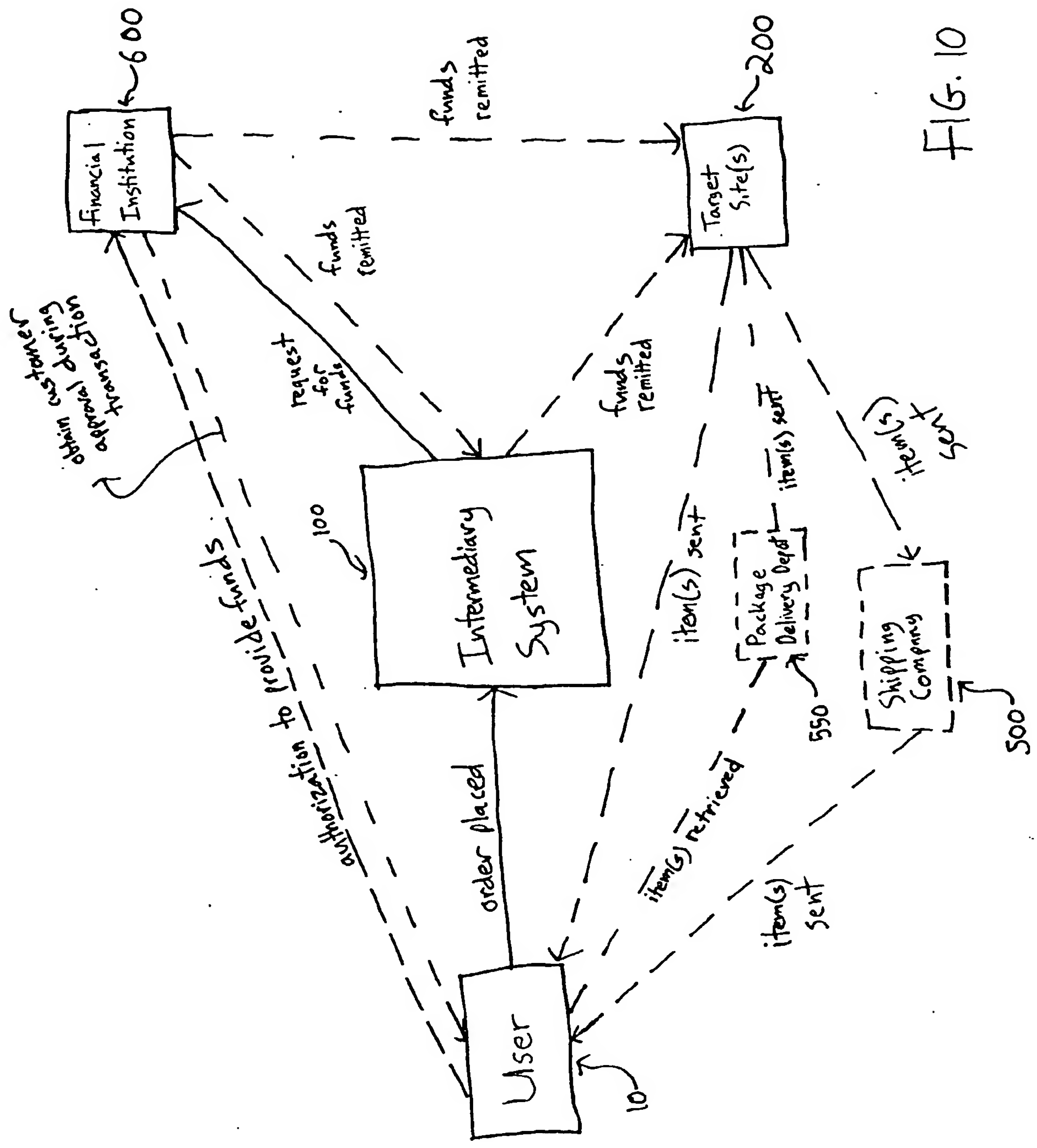

Financial Institution
600
Target Site(s)
200
Intermediary System
100
User
10
Package Delivery Dept
550
Shipping Company
500
funds remitted
funds remitted
funds remitted
request for funds
obtain customer approval during transaction
authorization to provide funds
order placed
item(s) sent
item(s) sent
item(s) sent
item(s) retrieved
item(s) sent

FIG. 10

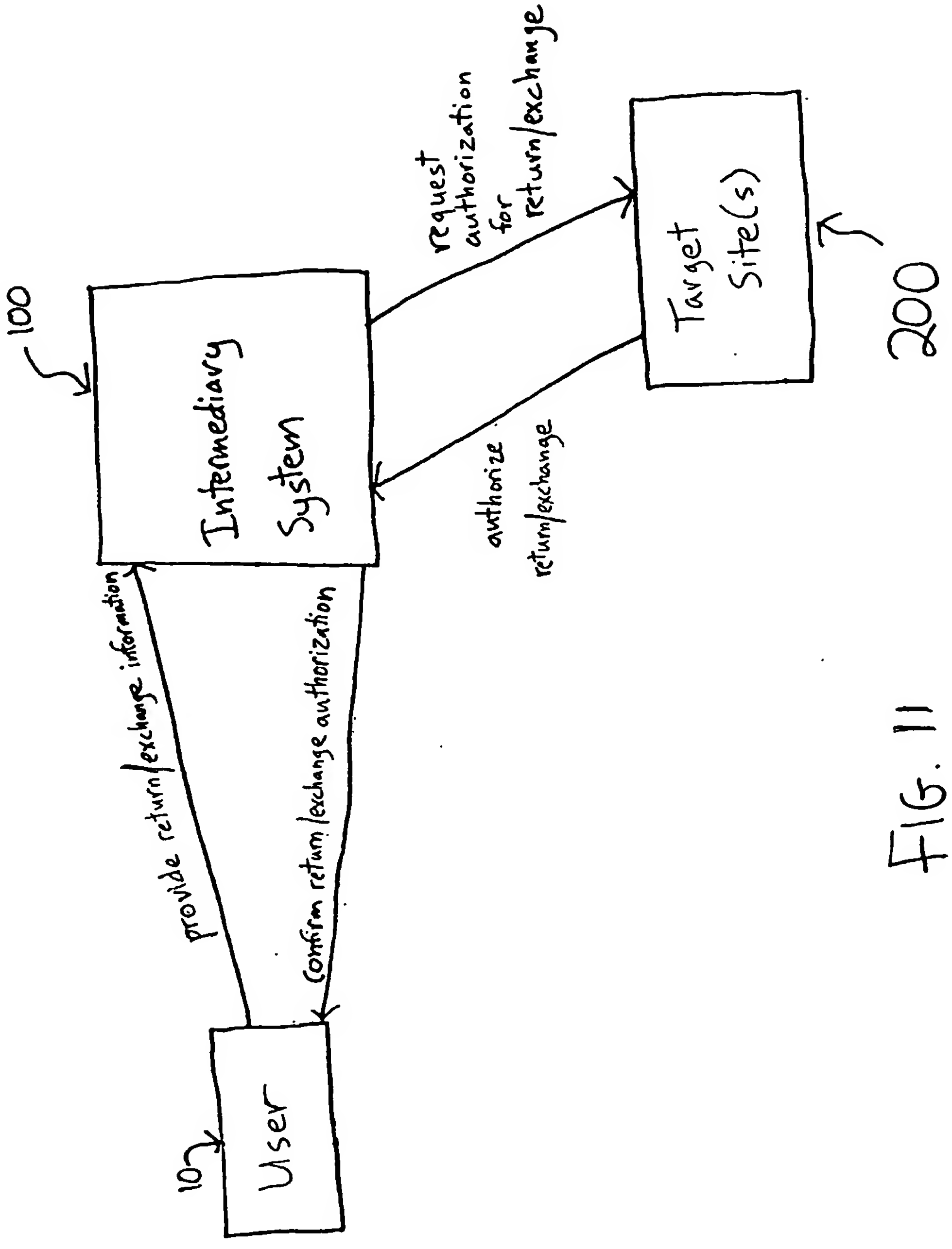

100
Intermediary System
request authorization for return/exchange
Target Site(s)
200
authorize return/exchange
provide return/exchange information
Confirm return/exchange authorization
10
User

FIG. 11

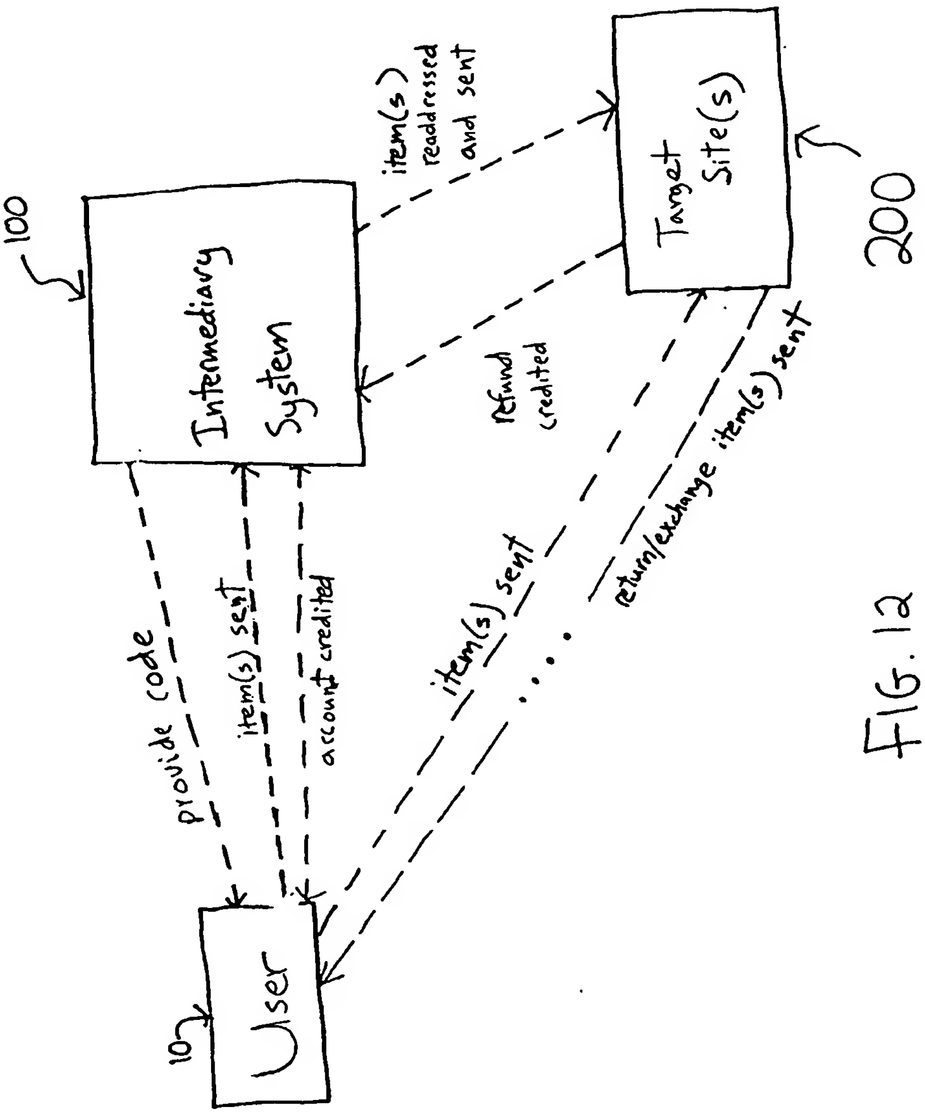

100
Intermediary System
Target Site(s)
200
item(s) readdressed and sent
Refund credited
provide code
item(s) sent
account credited
item(s) sent
return/exchange item(s) sent
10
User

FIG. 12

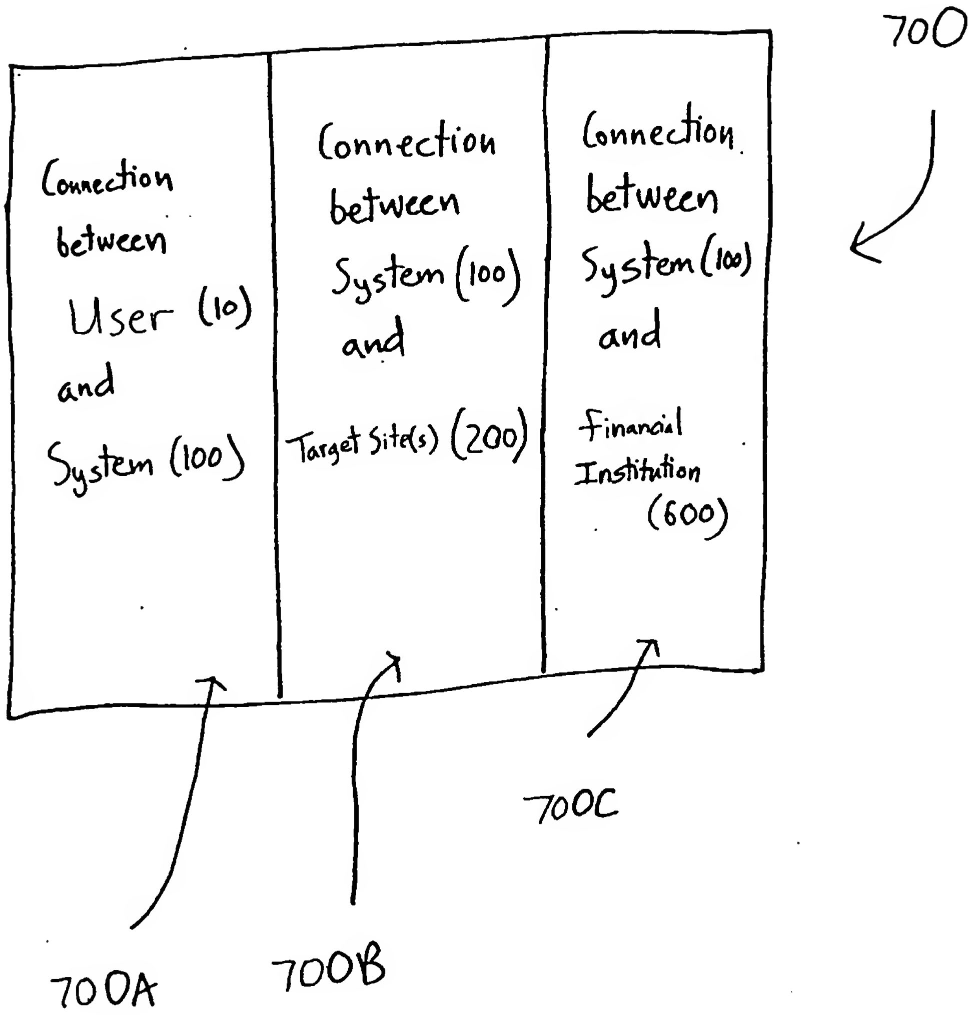

700
Connection between User (10) and System (100)
Connection between System (100) and Target Site(s) (200)
Connection between System (100) and Financial Institution (600)
700A
700B
700C

FIG. 13

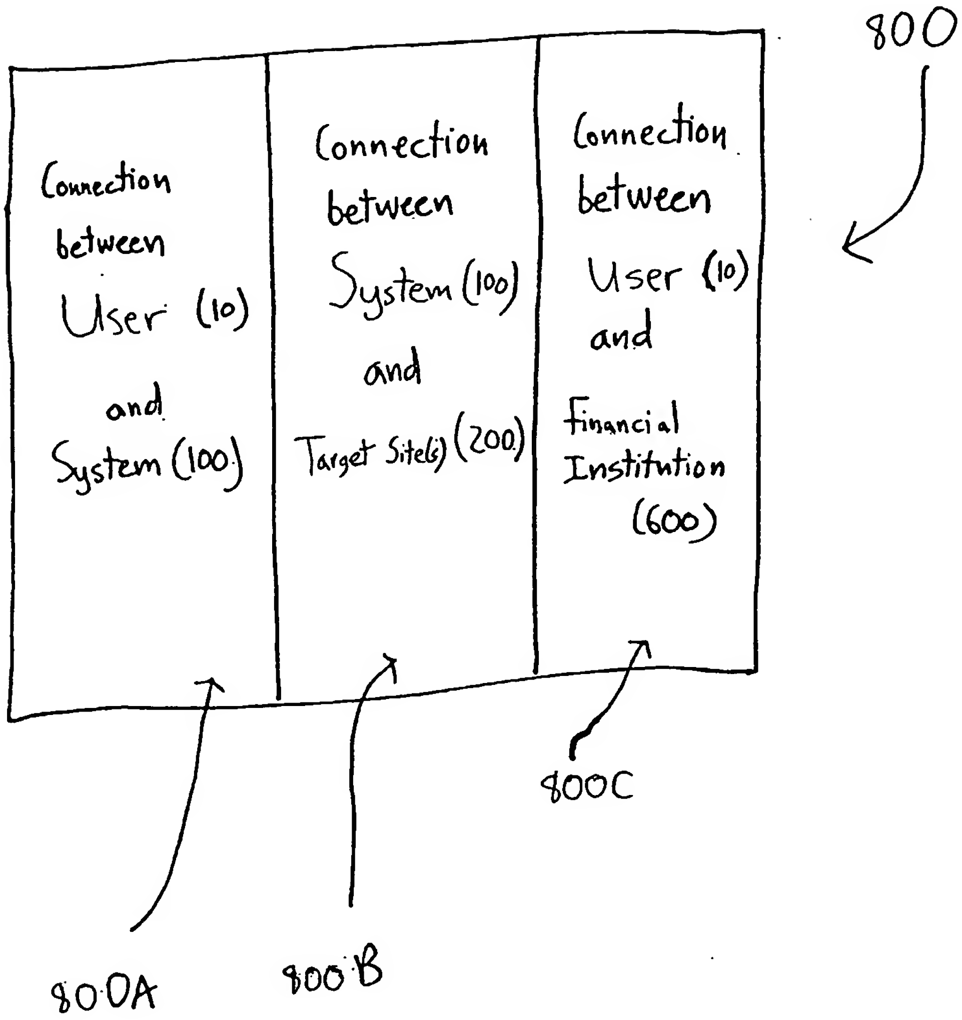

800
Connection between User (10) and System (100)
Connection between System (100) and Target Site(s) (200)
Connection between User (10) and Financial Institution (600)
800A
800B
800C

FIG. 14

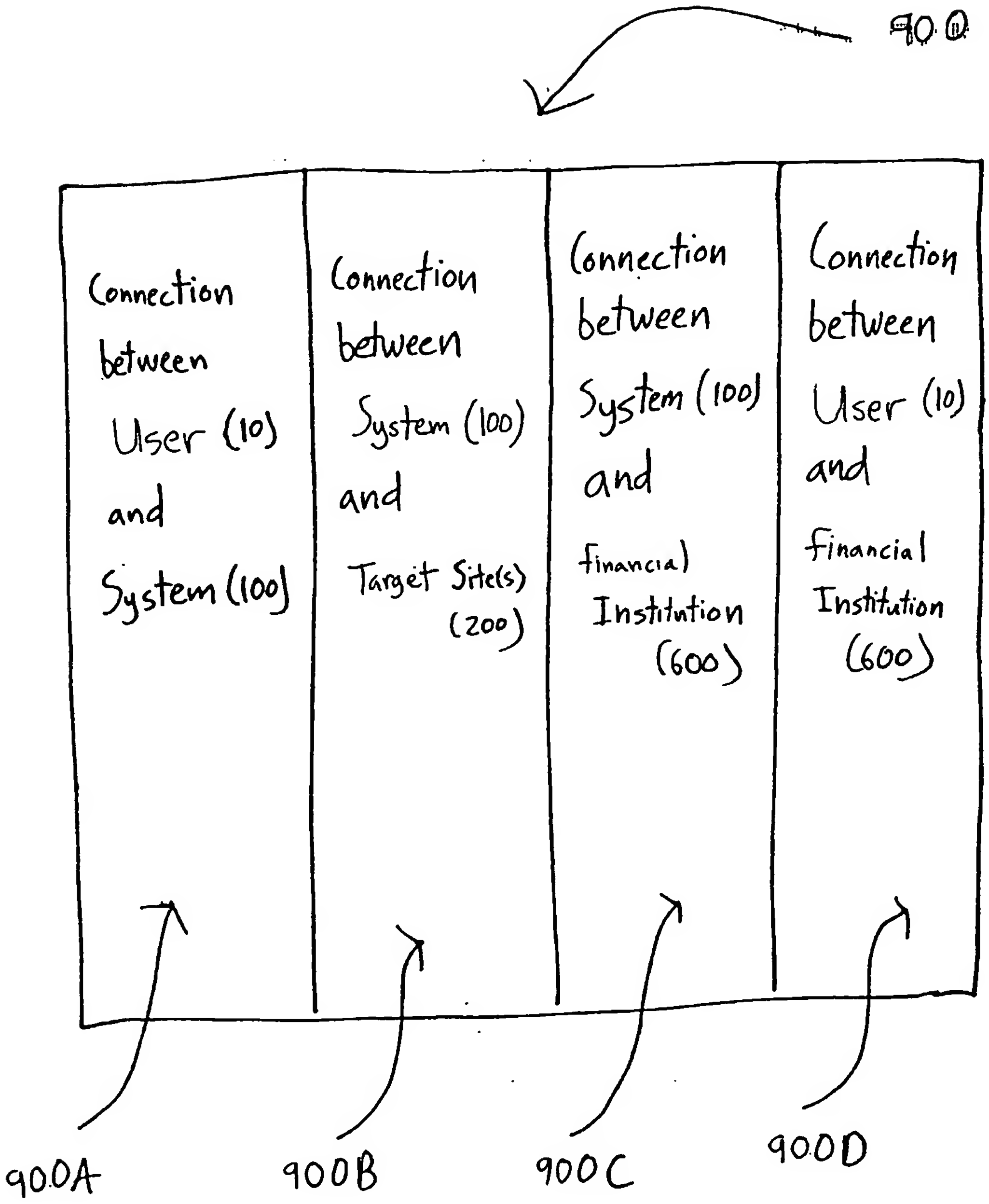

900
Connection between User (10) and System (100)
Connection between System (100) and Target Site(s) (200)
Connection between System (100) and financial Institution (600)
Connection between User (10) and Financial Institution (600)
900A
900B
900C
900D

FIG. 15